CAVERSHAM PARK PRIMARY SCHOOL

Online Safety Policy

CONTENTS

1. Introduction
2. Responsibilities
    i. Headteachers, Designated Safeguarding Lead and Senior Leaders
    ii. Online Safety Lead and Computing Curriculum Leader
    iii. Governors
    iv. Teaching and Support Staff
    v. IT support Provider
    vi. Learners
    vii. Parents and Carers
3. Acceptable Use
4. Reporting and Responding
    i. Reporting Concerns
    ii. Responding to Concerns
    iii. Recording and Monitoring
    iv. External Support and Escalation
    v. School actions
    vi. Responding to Learner Actions
    vii. Responding to Staff Actions
5. The Use of Artificial Intelligence (AI) in School
    i. Safe Use, Data Protection and Privacy
    ii. Quality Fairness and Integrity
    iii. Reporting Monitoring and Accountability
    iv. Use of Assessment and Feedback
    v. Misuse and Disciplinary Action
6. Online Safety Education Programme
    i. Digital Citizenship Curriculum
    ii. Internet Searching
7. Policy communication and training
    i. School Staff / Volunteers
    ii. Governors
    iii. Families
8. Technology
    i. Filtering and Monitoring
    ii. Technical Security
    iii. Cyber Security
    iv. Data Protection
9. Technical Practise
    i. Device Management
    ii. Digital Content
    iii. Public Online Communications
10. Outcomes

Introduction

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

This Online Safety Policy outlines the commitment of Caversham Park Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

Where online safety concerns or incidents occur outside school and are known to the school, Caversham Park Primary 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 as well as those that occur in school.

The Online Safety Policy has been developed using statutory guidance from Keeping Children Safe in Education (KCSIE). There are 4 types of online safety risks outlined in KCSIE:

- **CONTENT**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- **CONTACT**: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,
- **CONDUCT**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **COMMERCE**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is the responsibility of all staff to understand the above, recognise when a child may be experiencing harm related to the above, and report to the Designated Safeguarding Lead.

This policy should be read alongside other relevant school policies and procedures, including:

- Safeguarding Policy
- Behaviour and anti-bullying policies
- Code of conduct for staff and volunteers
- Acceptable Use Agreements
- RSHE Policy

The school will monitor and evaluate the impact of the policy using evidence, such as:

- logs of reported online safety incidents
- filtering and monitoring reports
- reviews of the effectiveness of the filtering systems
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of: learners; parents and carers staff.

The implementation and impact of the policy will be monitored and reviewed at regular intervals (at least annually) by the school leadership team and alongside the school's IT support provider. Anonymised details of online safety incidents will be reported to governors termly, through the Headteacher's Report.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff on how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by related acceptable use agreements
- is made available to staff at induction as part of the induction package
- is published on the school website.

It is important to recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- Schools have a duty to ensure that all children, young people and adults are protected from potential harm online.
- All staff and volunteers have a responsibility to help keep children and young people safe online, whether or not they are using the school's network and devices.
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

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, Designated Safeguarding Lead 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.

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding. The day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (the Headteacher), as defined in Keeping Children Safe in Education.

The Headteacher (and senior leaders in their absence) 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 Designated Safeguarding Lead /Online Safety Lead, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.

- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with governors, the Designated Safeguarding Lead, Online Safety Lead and IT provider on filtering and monitoring.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety, and understands filtering and monitoring systems and processes within their safeguarding role.

The DSL will:

- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with other members of 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.
- Review of the effectiveness on filtering and monitoring systems and ensure that these are recorded with the nominated SLT Lead and the IT provider lead the (at least annually).
- 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.
- provide (or identify sources of) training and advice for staff/governors

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

Online Safety Lead and Computing Curriculum Leader

The Online Safety Lead (OSL) support delivery of this policy; the DSL retains lead responsibility. The Online Safety Lead will:

- Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL).
- Lead development and review of online safety documentation.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.
- Work with curriculum leads to map, embed and evaluate online safety education.
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.
This will be provided through:

- a discrete programme
- the PHSCE / RSHE curriculum
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Governors

Governors are responsible for the approval of the Online Safety Policy and for challenging the effectiveness of the policy in line with KCSIE expectations.

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

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated.
- Ensure that children are taught about safeguarding, including in relation to online safety.
- Receive anonymised incident and monitoring summaries via the Headteacher's report to governors.
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard.

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

- Meet with the DSL/OSL.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review (at least annually), assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with DfE Filtering and Monitoring Standards.
- Report to the Full Governing Body
- Undertake basic cyber security awareness training and support school cyber security oversight.

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

Teaching and support staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.
School staff are responsible for ensuring that:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Information and Technical Security Policy and sign/comply with the Acceptable Use of IT and Social Media Agreement for Staff, Volunteers and Governors (AUA).
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues and that they immediately report any suspected misuse or problem to the Designated Safeguarding Lead / Online Safety Lead for investigation/action, in line with the school safeguarding procedures
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.

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

IT Support Provider

The IT provider supports school 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/ SLT / DSL
- Follow the school's Online Safety and Information and Technical Security Policy and keep technical knowledge current
- Support the school to ensure it meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body.

Learners

Pupils at Caversham Park Primary are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement, mobile phones in school policy, behaviour policy and Online Safety Policy. They should:

- 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 and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement and other relevant policies.
- seeking permissions concerning digital images and personal data
- parents'/carers' evenings, workshops, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices.

Acceptable Use:

The Online Safety Policy and acceptable use agreements define acceptable use at the school and this is shown in the tables below. The acceptable use agreements will be re-enforced through:

- staff induction
- posters/notices around where technology is used

- communication with parents/carers
- built into education sessions
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					**X**
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	through the use of computers/devices • Using penetration testing equipment (without relevant permission) NB: The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

User actions on school devices / network for non-educational purposes	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox,*	X				X			

Fortnite, Minecraft)								
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*			X		X			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)		X						X
Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*				X	X			
Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*			X		X			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*			X					X
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*	X				X			
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds)*		X			X			
Mobile phones used for learning (teacher-directed and supervised)	N/A				X			
Mobile phones used during social time/breaks (where permitted) including device-free approaches			X		X			
Taking photos/video/audio on devices (including sharing, location data and consent)				X	X			
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*			X		X			
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*		X			X			
Logging into personal accounts, e.g. gaming / Scratch	N/A				X			
School email used for personal communication (non-		X			X			

work/non-learning)								
Use of the laptop /iPad camera for taking photographs / making videos			X					X
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*	X				X			

Reporting and Responding

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting.

The school recognises 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. School staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child

Reporting Concerns

The school will ensure that:

- There are clear reporting routes which are understood and followed by all members of the school community.
- Reporting routes are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- 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.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online reporting tools (e.g., CPOMs), email contact, or in-person disclosures.

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.
- Any concerns about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the LADO.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring:

The school will:

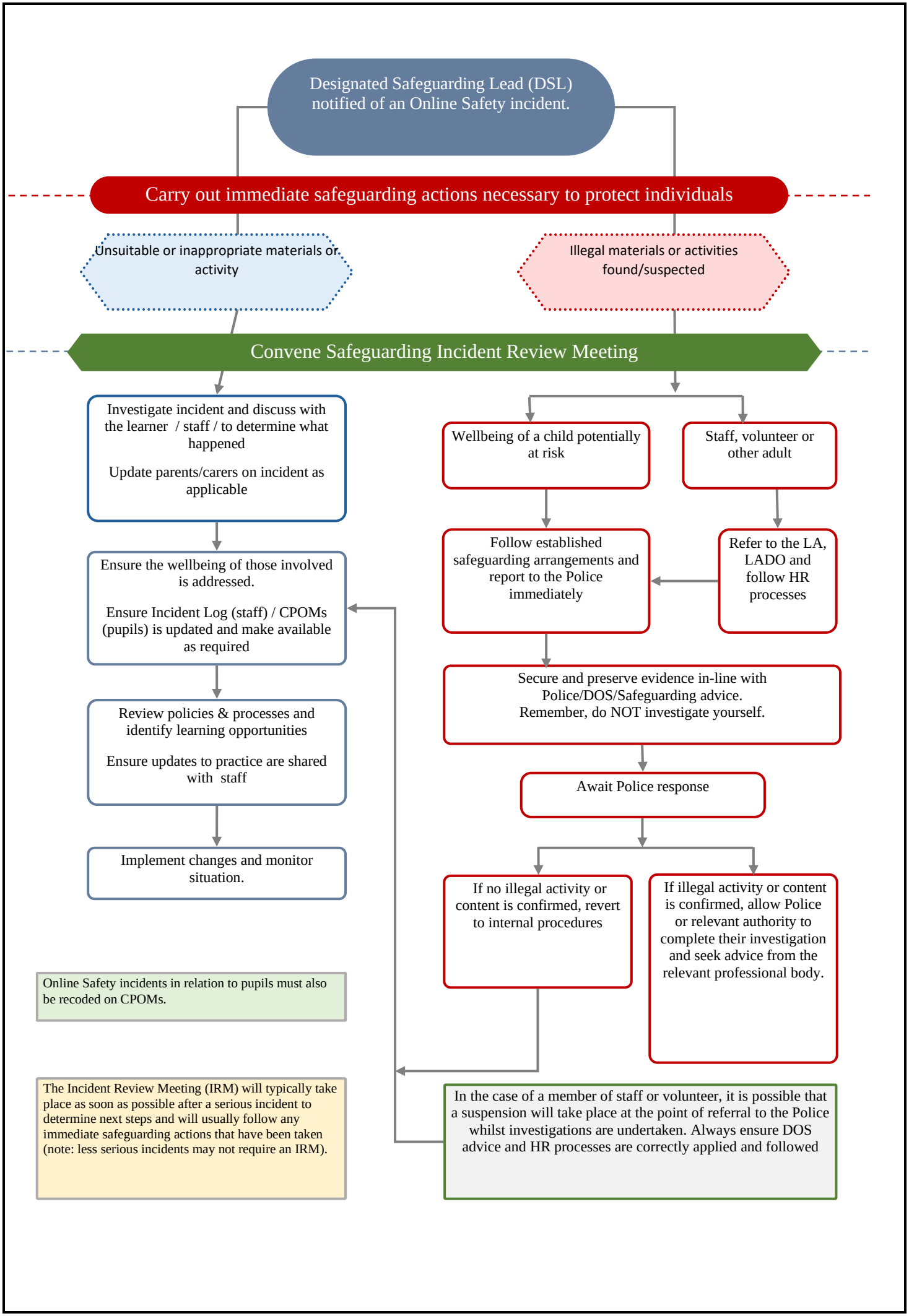
- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to: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

External Support and Escalation

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

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- UK Safer Internet Centre's Professionals Online Safety Helpline
- Reporting Harmful Content Service

The school will make the below flowchart available to staff to support the decision-making process for dealing with online safety incidents.


Designated Safeguarding Lead (DSL) notified of an Online Safety incident.
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log (staff) / CPOMs (pupils) is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.
Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
Online Safety incidents in relation to pupils must also be recoded on CPOMs.
The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

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 responded to. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to the computing / online safety lead.	Refer to Headteacher	Refer to Police/Social Work	Refer to technical support for advice/action	Inform parents/carers	Issue a warning	Remove device/ network/internet access rights	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).	inform	X	X	X		X	To be decided upon investigation and in line with incident history.		
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.	inform	X	X			X			
Damaging corrupting or destroying the data of other users.	X	X			X	X			
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Unauthorised downloading or uploading of files or use of file sharing or distribution.	X	X			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
Deliberately accessing or trying to access offensive or pornographic material.	inform	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X				X
Unauthorised use of digital devices (including taking images, videos and audio recordings) using a smart device in school.	X	X	X			X
Unauthorised use of online services, e.g. apps, websites or platforms.	X	X				X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	inform	X	X			X
Continued infringements of the above, following previous warnings or sanctions.	inform	X	X			X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority/ HR	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X		To be decided upon investigation.		

Actions which breach data protection or network / cyber-security rules.		X				To be decided upon investigation.
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	
Using proxy sites or other means to subvert the school's filtering system.	X				X	
Unauthorised downloading or uploading of files or file sharing	X				X	
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	X					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X			X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X	X			
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X	X			
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X				
Actions which could compromise the staff member's professional standing	X	X				
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X				
Failing to report incidents whether caused by deliberate or accidental actions	X					
Continued infringements of the above, following previous warnings or sanctions.		X	X			

The Use of Artificial Intelligence (AI) in School

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. Learners may be subject to harmful online interaction with other users or generative AI applications that simulate these and safeguarding of learners and staff remains central to our approach.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

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.
- 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 Privacy:

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 Headteacher / Online Safety Lead.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices.
- 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. Work must be anonymised.

Misuse and Disciplinary Action

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

See Use of AI in School 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.

Digital Citizenship Curriculum

The school has a broad, progressive, inclusive online safety education programme known as the Digital Citizenship Curriculum. This programme is planned for all year groups, builds on prior learning and is taught discreetly as part of the computing curriculum. This Digital Citizenship curriculum covers a range of skills and behaviours appropriate to their age and experience. As part of this pupils will be taught to:

- understand acceptable behaviour when using an online environment;
- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- know why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings;
- understand consent supported by safe opportunities for discussion;
- understand why they must not post pictures or videos of others without their permission;
- understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- understand how photographs can be manipulated;
- respect copyright and intellectual property, including when using online material and AI tools;
- develop strategies for dealing with receipt of inappropriate materials;
- understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying;

- to know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies.
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use

Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Internet Searching

The internet is an essential element of the 21st century life for education, business and social interaction. The internet is part of the statutory curriculum and a necessary tool for staff and pupils and the school has a duty to provide learners with quality internet access as part of their learning experience. The school internet access is designed expressively for pupil use and includes filtering appropriate to the age of the children. In order to ensure that the learners use the internet safely and responsibly school staff ensure that the following measures are in place:

- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit.
- Staff remind pupils about their responsibilities when using the internet and to encourage them to evaluate the information they access.
- Learners are taught how to report unpleasant internet content to a responsible adult.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and approved.

Policy Communication and Training

School Staff / Volunteers

In line with 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.

The school will ensure that:

- A planned programme of formal online safety, data protection and cyber security training is made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles

- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- staff follow cyber security policy and requirements.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings when necessary or changes are made.
- The Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- Attendance at training provided by the local authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Families

Families play an essential role in the monitoring/regulation of the children's online behaviours and in supporting their online safety education and wellbeing. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes;
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc. These provide information in relation to:
    - accurate, balanced and age-appropriate information about changes affecting social media and other online services
    - guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
    - guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- the learners - who are encouraged to pass on to parents the online safety messages they have learnt in lessons and by learners leading sessions at parent/carer evenings;
- letters, newsletters, the school website;

- high profile events / campaigns e.g. Safer Internet Day;
- reference to the relevant web sites/publications,
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches

Technology

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

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance and best practice guidance.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Checks on the filtering and monitoring system are carried out by the Online Safety Leader with the support of the IT Service Provider, senior leaders, the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- Where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products.
- The technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI generated content.
- Governors review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- Filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.

- Log reports provide actionable information for safeguarding decisions.

See Filtering and Monitoring Policy

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 with two-factor identification used where available and required
- 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.

See Information and Technical Security Policy

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 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue

The school ensures:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks; their safeguarding implications 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 s part of the cyber response plan.
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

See 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.
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

See Data Protection Policy

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

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

Device Management

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

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- learners do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Behaviour and Mobile Phone policies (in line with the DfE statutory guidance)
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons

- staff model the school's requirements and use personal devices only where authorised and professionally appropriate
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

Decisions about device use are reviewed regularly.

Digital Content

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

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations
- the school's progress towards meeting the DfE digital and technology standards

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. 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

Approved by the Governing Body on: ***[Insert date]***

Policy Date	Review Date
September 2026	September 2027

This policy has been written using advice and templates from SWGfL and LGfL