

WOODLANDS PRIMARY SCHOOL, HEDGEHOGS, NURSERY AND SUNBEAMS CLUB



ONLINE SAFETY POLICY Including AI

Updated: September 2026

Review Date: September 2027



Woodlands Primary School, Hedgehogs, Nursery and Sunbeams Club Staff and visitors Online Safety Policy



Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet, AI and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access and strong cybersecurity protections at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately, securely, and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Woodlands Primary, Hedgehogs, Nursery and Sunbeams club (the school) Online Safety policy which includes AI, cyber security incident response plan (see separate document) and the filtering and monitoring that is in place should help to ensure safe, secure, and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education - from the Headteacher and governors to Senior Leaders, classroom teachers, support staff, and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content, including through AI
- Unauthorised access to/loss of/sharing of personal information (data breaches, identity theft, cyber attack)
- The risk of being subject to grooming by those with whom they make contact on the internet (CSE & Prevent)
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication with others, including strangers
- Cyber-bullying / Mobile Phone bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Cybersecurity threats such as hacking, phishing, ransomware, and malware that target personal devices and school networks
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Using AI incorrectly

Many of these risks reflect situations in the offline world, but cyber security introduces additional challenges that require strong technical controls (such as firewalls, secure passwords, encryption, and monitoring systems) alongside digital literacy education. It is essential that this Online Safety and the cyber security incident response plan is used in conjunction with other school policies (e.g. Behaviour for Learning, Anti-Bullying, Acceptable Use, Safeguarding policies, Social Media Policy and cyber security incident response plan).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence, knowledge, and cyber security skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety policy and cyber security incident response plan that follows explains how The School intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible, informed, and secure users who can stay safe while using the internet and other communications technologies for educational, personal, and recreational use.

Development

This Online Safety policy has been developed by a working group made up of:

- School Computing Lead
- Headteacher and Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

The school will annually monitor the impact of the policy using:

- Logs of reported incidents via CPOMs (using E-Safety or Filtering and Monitoring category)
- Internal monitoring data for network activity
- Logs of inappropriate internet searches that have been flagged up
- Recording of daily Netsweeper report showing searches from both staff and children each day

Scope of the Online Safety Policy

This policy sets out how the school will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and student teachers. 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, this includes mobile phones and Smart watches. Staff are not permitted to use their own iPad, laptops or Chromebook on the school network. However, student teachers can as they have access to a separate network with more limitations.

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

Policy and leadership

Responsibilities

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

Governors

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

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

The governing body will nominate a Safeguarding Governor, which will including online safety, who will:

- Meet regularly with the DSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee.
- Undertake basic cyber security awareness training and support school cyber security oversight (all governors to have cyber security training each year).

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

Designated Safeguarding Lead (DSL)

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to be explicit in the DSL's job description.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Safeguarding Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the IT provider lead the (at least annually) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring).
- Ensure appropriate support for learners with SEND.

Online Safety/Computing Lead (OSL)

The OSL/Computing Lead will:

- Draft, review and monitor the Online Safety Policy and related documents for example cyber security plan and filtering and monitoring guide.
- 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.
- 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 and staff and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions.
- Send updates to staff and governors about Online Safety.

Curriculum Leads

Curriculum leads will work with the DSL/OSL to deliver a planned online safety programme (the school uses Common Sense Media) through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, police visits, assemblies and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff

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

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Cyber Security Plan and sign/comply with the Staff AUP (See Appendix 1).
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to computing lead.
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.
- See appendix 2 for information on Filtering and Monitoring.

Learners will:

- Follow the Learner AUP (See Appendix 3), recapped at the start of each term, Online Safety Policy and mobile phone policy.
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use internet responsibly: protect original work, check accuracy and avoid plagiarism.
- Any AI use will be age appropriate, used through an approved tool and be appropriately supervised by staff at all times.
- 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 Acceptable Use Policy for children is included in the welcome packs and are given to parents to sign when they start at Woodlands. These are then kept on file until the child leaves the school.

The school will:

- Publish the Online Safety Policy and share the learner AUP, which parents must sign.
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, Seesaw/Tapestry, emails or the school website.
- Share the online safety curriculum via school's website.

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

Community Users and Student Teachers:

Community Users, visitors and student teachers, who access the school ICT systems and Wi-Fi will be given access to a separate school network. This has limitations of what they can access compared to the staff at the school. Before accessing this network, they will be expected to sign a Staff User AUP before being provided with access to school systems.

In order for them to be able to access the schools Wi-Fi, they will be given a guest Wi-Fi password and code, this will be accessible for their length of stay within the school. Guest must agree and tick to give consent, to the following terms and conditions before being able to sign into the Wi-Fi:

- I agree to use the schools Wi-Fi for professional and educational use only.
- I agree that I will not use the schools Wi-Fi for personal use, social media use or to download inappropriate data.
- I understand that any inappropriate wording may be monitored and reported to SLT.
- The wireless network is provided "as is" without warranties of any kind, either expressed or implied.
- I agree not to use the wireless network for any purpose that is unlawful and take full responsibility of my acts.

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour for Learning, 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.

Online Safety Risks – The 4 C's

The school recognises the four categories of online safety risk:

- **Content:** Exposure to harmful, inappropriate or upsetting material.
- **Contact:** Contact with people who may pose a risk to children.
- **Conduct:** Online behaviour that may cause harm to others or themselves, including cyberbullying.
- **Commerce:** Risks associated with online financial activity, including scams, phishing and in-app purchases.

These risks are addressed through safeguarding procedures, filtering and monitoring, acceptable use policies and age-appropriate online safety education.

Implementation, monitoring and review

- This policy will be reviewed annually or sooner if a significant incident, new technology or change in guidance warrants it.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity.
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUPs and awareness activity.
- Published on the school website.
- Staff briefed on updates via staff meetings, training, inset days or Cheshire Police visits.

Acceptable use

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

Reinforcement

- staff and learner 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

Acceptable/Unacceptable Actions for both staff and children

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	- Fraud and financial crime (including money laundering) <i>Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).</i>					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	- Misusing someone else's username/ID or password to access data, software or systems without authorisation - Gaining unauthorised access to school networks, data or files (including bypassing security controls) - Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) - Phishing, credential theft, or attempting to capture passwords or personal data - Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) - Disabling, impairing or disrupting network/services (e.g., denial of service) - Using penetration-testing tools without explicit permission <i>Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime and into positive pathways.</i>					✓
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			✓	✓	✓

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	Promoting discrimination, harassment or hateful content				✓	
	Using school systems to run a private business or make unauthorised financial gain				✓	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				✓	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				✓	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			✓	✓	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				✓	

For non-Educational Purposes

	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (e.g. Roblox, Fortnite, Minecraft) N/A at The School	✓				✓			

Online shopping and digital commerce (<i>including in-app purchases, marketplaces, subscriptions</i>)			✓		✓			
Cloud storage and file sharing (<i>e.g., Google Drive, OneDrive</i>)		✓					✓	
Social media and user-generated platforms (<i>e.g. Facebook</i>) and other age-restricted services				✓	✓			
Messaging, chat and voice (<i>e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts</i>) <i>Staff have work related WhatsApp groups.</i>		✓ work related only			✓			
Streaming entertainment/media (video, music, podcasts) <i>e.g. Netflix, Disney+, Spotify</i>			✓		✓			
Video platforms and livestreaming (<i>e.g. YouTube only and for educational value. Live assemblies for topics and subjects</i>)			✓		✓			
Personal mobile phones and smart devices on site (<i>phones, smartwatches, earbuds, must follow separate policy</i>)			✓		✓			
Taking photos/video/audio on devices (including sharing, location data and consent) <i>These are school devices only and must follow the photo guidance.</i>	✓							✓
Other personal devices (<i>e.g., tablets, handheld consoles, VR headsets, wearables</i>)	✓				✓			

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. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child and record via CPOMS.

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 and 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 and added to CPOMS, 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, OSL, 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.
- 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
 - Local safeguarding partners where relevant

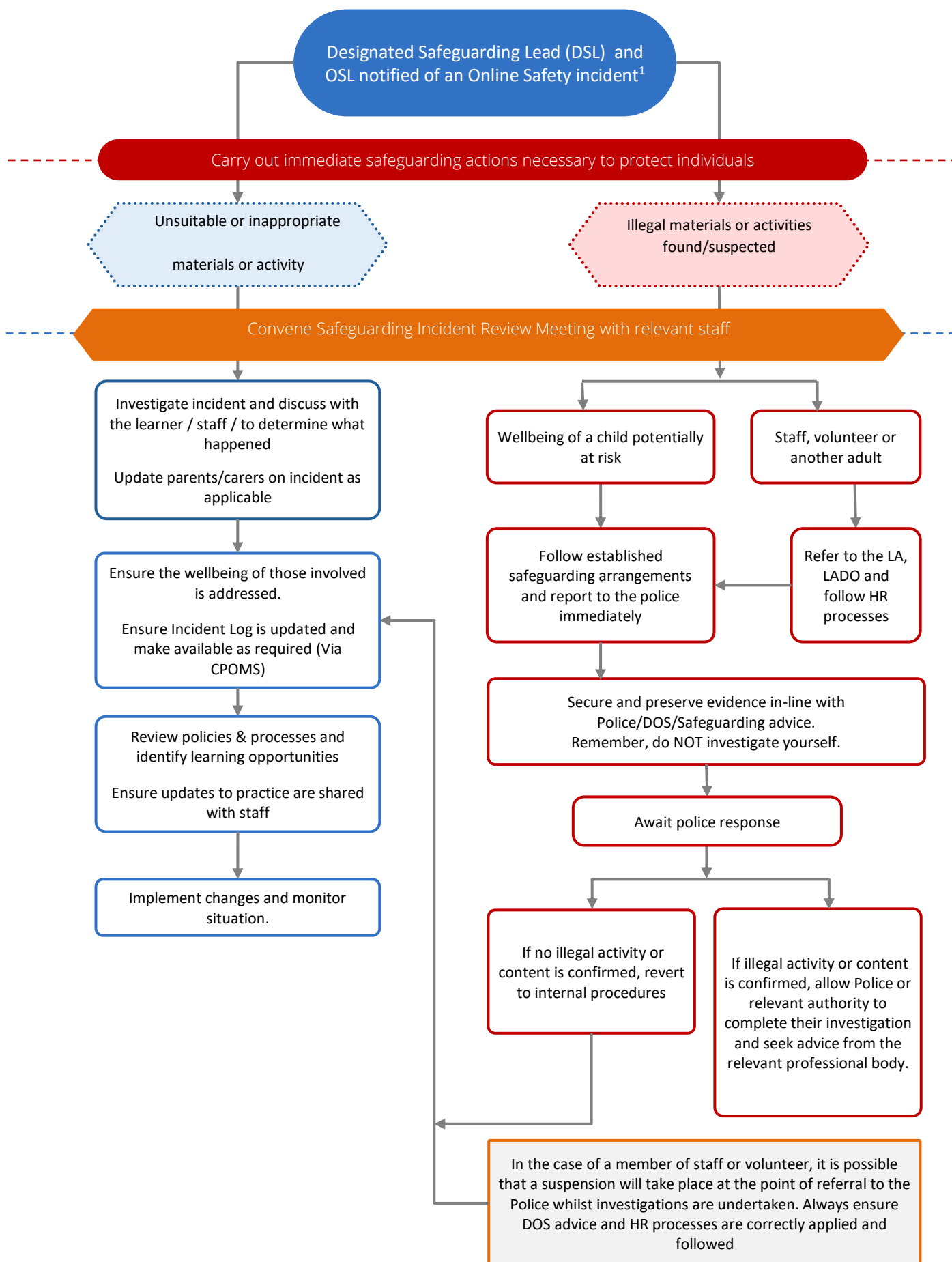
External Support and Escalation

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

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

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

This flowchart should be followed to support the staff decision-making process for dealing with online safety concerns.



Incidents	Refer to class teacher/tutor	Refer to DSL / OSL	Refer to SLT	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier “Unsuitable/Inappropriate Activities” section.		✓	✓	✓		✓			✓
Unauthorised access to the school network , including using another person’s account or sharing usernames/passwords.	✓	✓	✓			✓			✓
Damaging, corrupting or deleting another user’s data.	✓	✓	✓			✓			✓
Sending offensive, harassing or bullying emails, texts or messages.	✓	✓	✓		✓	✓			✓
Unauthorised downloading/uploading , file sharing or distribution of files.	✓	✓	✓	✓	✓	✓			✓
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	✓	✓	✓	✓	✓	✓			✓
Failing to report accidental access to offensive or pornographic material	✓	✓	✓	✓	✓	✓			✓
Deliberately accessing offensive or pornographic material (or attempting to)	✓	✓	✓	✓	✓	✓			✓
Sharing or receiving content that breaches copyright or data protection law.	✓	✓	✓	✓	✓	✓			
Unauthorised use of devices , including taking photos/videos or	✓	✓	✓						

audio recordings and using a smartphone in school									
Unauthorised use of online services (apps, websites or platforms).	✓	✓	✓						
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	✓	✓	✓	✓					
Repeated breaches of these rules following previous warnings or sanctions.	✓	✓	✓						

Responding to Staff Actions

Incidents	Refer to line manager	Refer to SLT / Headteacher	Refer to MAT / LA	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	✓	✓	✓	✓	✓	✓	✓
Breaching data protection or cyber-security requirements , including network security rules.	✓	✓	✓	✓	✓	✓	✓
Accessing offensive or pornographic material (or attempting to).	✓	✓	✓	✓	✓	✓	✓
Damaging systems or data , including corrupting/deleting others' data or deliberately damaging hardware/software.	✓	✓	✓	✓	✓	✓	✓

Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	✓	✓			✓		
Unauthorised downloading, uploading or file sharing.	✓	✓			✓		
Breaching copyright, licensing or intellectual property , including misuse of AI systems.	✓	✓			✓		
Unauthorised account/network access , including sharing passwords, using another person's account, or allowing others access.	✓	✓			✓		
Sending offensive, harassing or bullying emails, texts or messages.	✓	✓	✓	✓		✓	✓
Use of personal email/social media/messaging to communicate with learners or parents/carers.	✓	✓				✓	✓
Inappropriate personal use of school technology , including personal email and social media use during work time/using school systems.	✓	✓				✓	✓
Mishandling personal data , including storing, displaying or transferring it insecurely.	✓	✓				✓	
Any action that undermines professional conduct or a staff member's professional standing.	✓	✓				✓	✓
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	✓	✓				✓	✓
Failing to report incidents , whether accidental or deliberate.	✓	✓				✓	✓
Repeated breaches following previous warnings or sanctions.	✓	✓				✓	✓

Education

Online Safety Education Programme

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

The school delivers a 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". Common Sense Media curriculum has been implemented which is used from Reception through to Year 6. Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship) and has clear intended outcomes. These lessons are taught once per half term as a stand-alone lessons and the key themes are then reinforced through starters during computing lessons. To support the curriculum, age-appropriate stories are also shared with the children throughout each half term, helping to develop their understanding and reinforce key learning.

In addition to the above, Digital Literacy units are being introduced in the Spring term to help children develop a deeper understanding of keeping safe online and AI. Special days are also celebrated and the children carry out discussion and activities on Safer Internet Day (February) and AI awareness day (June).

Workshops and assemblies take place throughout the year on keeping safe online and cyber security. Reception children take part in three 'Cyber Sid' sessions. All workshops are delivered via Cheshire Police.

Online safety displays are displayed throughout the school, in classrooms and computing suites.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries.
- 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
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where computing and 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. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale. Teachers will monitor KS2 children on the internet by using Classroom Cloud for the laptops and Chromebooks or Veygon when in the computer room. Key stage 2 staff have been trained to use these.

Pupil voice is actively used to strengthen the school's approach through feedback, learner representation, peer mentoring, campaigns, and contribution to acceptable use. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

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

All staff will receive online safety training and understand their responsibilities under this policy. Training will include:

- A planned programme of online safety, 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.
- 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 policy, 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. Posters explaining what to do if the school has a cyber attack are stored in each classroom, school office and computer rooms.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy, mobile phone policy and Acceptable Use Policy, 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, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources and, where appropriate, enhanced pathways.
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

Governors

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

Training and updates may be provided through:

- Attendance at training offered by the Local Authority or other relevant organisations (e.g. SWGfL).
- Participation in 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 OSL to review key themes, incidents and current priorities.

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

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

External Stakeholders

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

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

Working with Parents and Carers

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

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, Seesaw/Tapestry, 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). These are found on the school website and parents have regular reminders via Seesaw to access the school website.
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches. This policy is accessible on the school's website.
- accurate, balanced and age-appropriate information about changes affecting social media and other online services
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place

- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

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

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community via newsletters, Seesaw, Tapestry and the school website.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website, Seesaw and Tapestry channels to offer online safety content suitable for the broader community.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).

Use of Artificial Intelligence (AI)

Artificial Intelligence (AI), is increasingly used in education and everyday life. The school recognises its potential to enhance teaching and learning, improve outcomes, support assessment, reduce staff workload and improve school operations.

However, AI also presents risks, including safeguarding concerns, data breaches, inaccurate information, bias and discrimination. These risks will be managed through our existing safeguarding, data protection, online safety and technical security procedures, which will be reviewed as necessary.

We are committed to promoting the safe, ethical and responsible use of AI. The school will prepare staff and pupils to understand both the benefits and risks of AI, while keeping the safeguarding and wellbeing of children and staff at the centre of all decisions.

Policy Statements

Appropriate use and accountability - AI may be used purposefully to support teaching and learning, assessment, feedback, administration and workload reduction. Staff remain professionally responsible for all AI-assisted work, decisions and outcomes. AI must support, not replace, professional judgement.

Approved tools and data protection - Staff must use only school-approved AI platforms: ChatGPT, Gamma and Canva Education. School email addresses must be used to register for and access these accounts. All use must comply with UK GDPR, the Data Protection Act 2018 and relevant safeguarding guidance. Staff must use anonymised data wherever possible and must not enter their own or pupils' personal information, sensitive data, confidential documents or internal school information into AI tools unless the tool and purpose have been explicitly authorised and meet the school's data protection and security requirements.

Accuracy, fairness and human oversight - AI-generated content must be checked for accuracy, reliability, bias and discrimination before it is used, shared or published. Decisions affecting pupils, staff or other individuals must remain under human control.

Copyright and transparency - Staff must respect copyright, intellectual property and the rights of pupils and colleagues. Where AI has materially contributed to documents, presentations, communications or other work, its use should be clearly acknowledged where appropriate.

Training and education - The school will provide staff and governors with appropriate training and guidance on the benefits, risks and responsible use of AI. Further training needs will be identified and addressed when appropriate.

Through age-appropriate teaching in computing, online safety and PHSE lessons, alongside the annual AI Awareness Day in June, pupils will develop an understanding of how AI works, its uses, benefits, limitations, ethical implications and potential risks. They will learn how to approach AI safely, responsibly and critically.

Pupils must not independently access or use AI tools in school. Any pupil use of AI must be authorised by the school, age-appropriate, comply with the tool's minimum-age requirements and take place under direct staff supervision using an approved platform.

Safeguarding and inclusion - The school will consider the safeguarding, wellbeing and accessibility implications of AI, recognising that some pupils may be more vulnerable to its misuse. Existing safeguarding, online safety, filtering and monitoring arrangements will support the safe use of AI.

Monitoring and risk assessment - The school will maintain an inventory of approved AI tools, recording their purposes and associated risks. AI use will be reviewed regularly. New or changing risks will be addressed through the school's existing procedures.

Reporting and accountability - Staff must promptly report AI misuse, inappropriate outputs, suspected data breaches or other AI-related concerns to the Senior Leadership Team (SLT) and Online Safety Lead (OSL), following established school procedures. Safeguarding concerns must also be reported to the Designated Safeguarding Lead (DSL), in line with the school's safeguarding procedures.

Incidents will be recorded and managed in line with safeguarding, data protection and disciplinary procedures.

Consequences of misuse - Failure to follow this policy, including the misuse of AI or breaches of data protection requirements, may result in disciplinary action in accordance with the school's Staff Disciplinary Policy.

Use of AI in Teaching, Learning and Assessment

AI may be used to support teachers with planning, resource creation, assessment, identifying areas for improvement and drafting feedback. It may also support pupils in developing and improving their work where appropriate.

All use must have a clear educational or professional purpose. Teachers remain responsible for the accuracy, fairness and suitability of AI-generated content and feedback, ensuring that it meets pupils' needs and supports their understanding and progress.

AI must not replace teachers' professional judgement or make significant decisions about pupils without appropriate human oversight. Any use of AI in assessment must follow relevant school procedures and applicable assessment requirements.

Responsibilities

Headteacher and Senior Leadership Team

- Oversee the school's approach to AI and ensure that this policy is implemented.
- Ensure staff understand the policy and receive appropriate training.
- Review AI-related risks and ensure concerns are addressed.

Designated Safeguarding Lead and Online Safety Lead

- Understand the safeguarding implications of AI and relevant guidance.
- Support staff in identifying and reporting AI-related safeguarding concerns.
- Ensure incidents are managed through established safeguarding procedures.

Data Protection Officer

- Advise on data protection requirements, the safe use of AI and the need for Data Protection Impact Assessments (DPIAs).

Technical staff and Computing Lead

- Support the safe use of approved AI tools.
- Consider cybersecurity, filtering, monitoring and technical risks.

All staff

- Read and follow this policy and relevant Acceptable Use Agreements.
- Use AI responsibly and protect personal, sensitive and confidential information.
- Check AI-generated content before using or sharing it.
- Report concerns promptly and maintain professional accountability.

Governors

- Understand the benefits and risks of AI in school.
- Receive appropriate training and updates to support oversight and challenge where necessary.

Parents and carers

- Be provided with appropriate information about how AI is used in school and guidance on its benefits and risks.
- Be encouraged to raise any concerns through the school's established reporting arrangements.

Reporting and Responding to Incidents

All AI-related concerns, including misuse, harmful or inappropriate outputs, safeguarding concerns and suspected data breaches, must be reported promptly through the school's established procedures.

The school will:

- Respond to concerns promptly, sensitively and in accordance with safeguarding and data protection procedures.
- Record incidents using the school's normal recording systems.
- Refer incidents to external agencies where required.
- Follow normal staff disciplinary procedures where staff misuse AI.

Review

This policy will be reviewed regularly and updated when necessary to reflect changes in AI technology, relevant legislation, safeguarding guidance and school practice.

Technology

Purpose

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

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance and best practice guidance. The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring when connected to the school network.
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- 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
- The school will consider AI-enabled features within websites, apps, browsers and other digital services when reviewing filtering and monitoring arrangements.
- The school will assess the safety, age suitability, moderation and filtering capabilities of AI tools before approving them for educational use.
- The school recognises that filtering and monitoring systems may not identify every harmful AI-generated output. Staff supervision, clear reporting procedures and professional judgement remain essential.

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions. The staff, children and visitors all have different levels of permissions.
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise

- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the [DfE Cyber Security Standards](#) and recognises cyber security as a safeguarding issue).

The school ensures that:

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

See separate cyber security policy and plan for further details.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

The school ensures that:

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

Review

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

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

Technology Practice

Purpose

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

This approach supports the safeguarding duties set out in KCSiE 2026, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

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

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSiE 2026's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education. (See separate policy).

The school ensures that:

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

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

Digital Content

The school recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content

- personal data and images are handled securely and lawfully
- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.
- Pupils and staff must not use AI to create, alter or share images, videos, audio or other content involving another person in a misleading, humiliating, threatening or harmful way. Any suspected AI-generated abuse, impersonation or non-consensual intimate imagery must be reported immediately through the school's safeguarding procedures. Staff must not forward or copy suspected illegal images.

Public Online Communications

The school uses Seesaw and Tapestry to inform and engage with parents and carers about successes in their child's learning and celebrate achievements in school. 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 and staff will follow these guidelines when taking photos in school.

- Avoid using close-up photos or images that clearly show children's full faces.
- Use images that are harder to misuse. This includes taking photos from a distant, different angles, group photos or photos of the children working, over their shoulder.
- Avoid taking images that show easily identifiable features such as birthmarks.
- Where possible, use photos of children's work, certificates or displays
- Removing photo metadata (such as timestamps and location information).
- Use school owned devices to take photos and not personal mobile phones.

Parents are aware of these changes and also know that they can opt out of photo permission at any points whilst their child is at the school.

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.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks

- feedback from staff, learners and parents
- national guidance and statutory expectations
- the school's progress towards meeting the DfE digital and technology standards
- the impact of mobile-phone arrangements and changes affecting children's access to online services.

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



Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club Staff and visitors Acceptable Use Policy



New technologies are now a big part of most people's lives, both in and out of school. The internet, AI and other digital tools offer many new opportunities for learning and communication. They can help spark discussion, boost creativity, and support better learning for all. These tools also help teachers work more creatively and efficiently. It is vital to keep staff, governors, children and school visitors safe at Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club (the school) as well as the schools IT systems and devices. This Acceptable Use Policy, when followed, will help to keep everyone safe as well as the schools IT systems and users protected from mistakes or misuse that could cause problems or security risks.

Scope

This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- email systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- computing devices – *this covers ANY computing device used for work purposes, whether at the place of work, home or elsewhere*
- photocopying, printing and reproduction equipment
- documents and publications (any type or format)

Acceptable Use Policy Agreement

The school is committed to providing staff and volunteers with good access to ICT to support their work both in and out of school, and to enhance pupils' learning. In return, the school expects all staff and volunteers to use ICT responsibly by agreeing to and following the guidelines outlined below.

Use of Artificial Intelligence (AI)

Staff must use AI safely and responsibly, following the school's AI Policy.

- **Approved tools:** Only use school-approved AI tools: ChatGPT, Gamma and Canva Education. Use your school email address to access these accounts.
- **Protect information:** Never enter pupils' personal details, photographs, SEND or safeguarding information, or confidential school information into AI tools unless specifically authorised by the school.
- **Check the content:** Always check AI-generated text, images and resources for accuracy, bias and suitability before using or sharing them.
- **Take responsibility:** AI can support teaching, planning, assessment and administration, but staff remain responsible for all work and decisions. AI must not replace professional judgement.
- **Assessment:** Do not rely on AI alone to assess pupils or make decisions about their learning, needs or wellbeing.
- **Safeguarding:** Never use AI to create or change images, videos or other content in a harmful, misleading or inappropriate way.
- **Copyright:** Respect copyright and the rights of others when using AI-generated materials. Acknowledge AI use where appropriate.
- **Sharing and publishing:** Check AI-assisted letters, reports and other communications before sharing them.
- **Pupil use:** Pupils must not independently access or use generative AI tools in school. Any use of AI by pupils must be specifically authorised by the school, age-appropriate, comply with the tool's minimum-age

requirements and take place under direct staff supervision using an approved platform. Staff will teach pupils about AI, including its benefits, limitations and potential risks, as part of the online safety and computing curriculum.

- **Report concerns:** Report any misuse of AI, inappropriate content, safeguarding concerns or possible data breaches promptly through the school's reporting procedures.

Computer Security and data Protection

- Every staff member will get their own school computer account with a personal username and password that must be used for school related communication only. This account will match the level of access they need and should not be shared.
- Passwords must be strong. Use three random words with capital letters, numbers, and symbols. Never share your password with anyone and they should not be kept near or on any computing device.
- Passwords for any school device (computers, laptops, iPads, tablets etc) should not be given to children.
- Each laptop has a Bitcode for access. Staff must not store this Bitcode on or near their laptops
- Pupils must not use staff accounts or passwords. Staff must keep their login details secure and must not share them with pupils. Staff are fully responsible for any problems that happen as a result.
- When leaving a computing device unattended, staff must log out or lock the screen to stop others from accessing their account or emails.
- USB sticks or portable hard drives should not be used with the school system as they might have viruses. Staff must not save sensitive or personal data on these devices unless the school has approved and encrypted them.
- If staff use USBs on their home computers, they must make sure their home computer has updated antivirus software to prevent spreading viruses to the school network.
- If staff use a personal computer or device at home for school work, they must not store any sensitive or personal school data unless the device is fully encrypted by IT support and approved by the headteacher.
- The school server and emails are backed up every night. Staff should regularly back up files from their Desktop and Downloads folder, as these may not be included.
- It is the responsibility of the staff to ensure laptops, tablets, iPads, cameras, and other school devices are locked away at the end of the day and not left where they can be seen through windows or doors.
- Do not click on links or open attachments from unknown or untrusted email sources. Report any suspicious, harmful, or inappropriate content or emails right away to IT support or the Computer Lead.
- In the event that your device is lost or stolen, you must inform the school immediately who will advise on the next steps.

Conduct

Staff must...

- Always use the school's computer system in a professional, polite, and legal way that does not harm the school's or their own reputation.
- Not access, use, download, or share illegal or harmful content, such as child abuse images, racist material, or pornography.
- Not use or share offensive, rude, racist, sexist, or threatening language or material or make jokes or comments about someone's race, gender, or sexual preference.
- Follow and respect the school's computer security rules and not try to get around them.
- Not damage or harm any school computer or device.
- Not download large amounts of data or store lots of personal files on the school system.
- Not access, copy, or change another person's files without permission.
- Only contact pupils, parents, or carers using school email accounts or systems, and always be professional. These communications should be recorded on CPOMS. Personal phones or email accounts must not be used.
- Pupil information must only be stored on approved, secure school systems. It must not be taken off school premises unless authorised and necessary for school business, and must be kept secure at all times.

- Ask IT support or Computer Lead if they want programs installed onto computing devices.
- Keep all pupil and staff data private, unless required to share by law or school policy.
- Have permission before using someone else's work and follow copyright rules. Music, videos, and other protected materials should not be copied or shared illegally.
- Be responsible for their actions, both in and out of school.

Mobile Phones

- Staff must not use their mobile phones when children are present. Phones must be switched off or on silent and kept out of sight, such as in a cupboard or bag, during the school day. The only exception is when a phone is needed in the classroom for two-step verification to access school emails.
- Staff must not charge their phones in the classroom. Phones can only be used in the PPA room or staff room during breaks or lunchtime, or with permission from the Headteacher or a senior staff member.
- Children must never be allowed to use staff mobile phones.
- Staff must not use personal phones to take photos or videos of children or to update Seesaw/Tapestry unless the Headteacher has given permission. If allowed, photos must be moved to the school computer system immediately and then deleted from the phone. However, if mobile phones are the only device available and are used to take photographs they should only be used in exceptional circumstances.
- If a member of staff needs to make an urgent personal phone call they can use their phone at an appropriate non-contact time. If a member of staff has a family emergency or similar and needs to keep their mobile phone to hand, prior permission must be sought from their phase leader.

Personal Use

The school allows staff to use school computers for personal reasons from time to time, as this can help improve IT skills and support a good work-life balance. This is allowed under the following conditions:

- Staff must still follow this Acceptable Use Policy and all other school rules for staff behaviour.
- Personal use must not slow down or affect the school's computer system.
- Staff laptops must not be used for business or commercial work unless the school gives permission.
- IT support monitors all computer use, whether it's for work or personal reasons. If you access private information, you do so at your own risk.
- Staff must not store personal files on the school system, including:
 - Music
 - Games
 - Videos
 - Photos or images

If these types of files are found, staff will be asked to delete them.

Photographs

- Staff must get permission before taking or sharing photos or videos of other staff or children, and must follow the school's rules on using digital images. If images are shared (e.g. on the school website), names or personal details will not be included.
- Photos shared on Seesaw or Tapestry will include a child's first name and first letter of their surname. Parents have been informed and have given permission for this.
- Staff can take photos or videos for educational purposes, but must follow school rules on how these are shared and used. Images should only be taken using school devices.
- Staff mobiles and personal devices must not be used to take photos of the children.

When taking photos of children, staff will:

- Avoiding using close-up photos or images that clearly show children's full faces.
- Using images that are harder to misuse. This includes taking photos from a distant, different angles, group photos or photos of the children working, over their shoulder.
- Avoiding taking images that show easily identifiable features such as birthmarks.
- Where possible, use photos of children's work, certificates or displays
- Removing photo metadata (such as timestamps and location information).

Smartwatches

- Staff are permitted to wear smartwatches at school; however, if the device includes a camera function, it must not be used to operate the camera—either directly or via a connected mobile phone—in accordance with the above guidelines on mobile phone use.

Supervision of Pupils

- Pupils must always be supervised when using school computers or mobile devices during lessons.
- Staff should regularly remind children about the Acceptable Use Policy to help keep them and the devices safe.
- Children must not use computing equipment without supervision during break or lunchtime.
- Staff can use 'School Cloud' or 'Vygon' to monitor pupils' work during lessons, and are encouraged to do so.
- All children's mobile phones must be collected at the start of the day and locked away safely. Phones are returned at the end of the school day. Children should not use them during school hours.
- Children should be informed that their computer use is being monitored. Any inappropriate internet searches will be flagged, and parents will be informed of any misuse.
- All staff should teach the children about how to use ICT and the internet safely whenever possible.
- Teacher tablets have staff access only. Children must be supervised when using these and use them at the risk of the teacher.

Use of Social Networking, Websites and Online Forums

Staff should be careful when using social media, even in their own time. Please follow these rules:

- Do not use social media during school time or on school devices.
- Do not add pupils as friends or message them privately on social media, even for school reasons.
- Be careful what you post online. Make sure your comments don't harm your professional reputation or that of the school.
- Unless you have permission, do not post anything that makes it seem like you are speaking for the school.
- Do not mention the school on social media in a negative or inappropriate way.

Use Of Your Own Equipment – Bring Your Own Device

- If you bring your own device to school, it's your responsibility. The school is not responsible for any damage or loss. When not in use, keep it in a safe place.
- Do not store school photos or videos that include staff or children on your personal devices like phones or tablets.
- Do not connect your personal devices to the school's computers or network without permission from IT Support.
- Any staff member, volunteer or student found to be non-compliant with this policy will face disciplinary action.



Filtering & Monitoring at Woodlands

A staff guide: what we use, and why

For all teaching and support staff | September 2026

1. Why we use these tools

As a school, we have a legal duty to do everything reasonable to keep pupils safe while they're using the internet and school devices, set out in Keeping Children Safe in Education (KCSIE) 2026. Filtering and monitoring are two of the main ways we meet that duty.

Understanding how they work is part of safeguarding induction and annual training for all staff, in the same way as knowing who the Designated Safeguarding Lead (DSL) is or what the child protection policy says. This guide sets out what's in place at Woodlands, why we use it, and - most importantly - what it means for your everyday practice in the classroom.

2. The two tools we use

We use two systems together because they do different jobs: one stops pupils reaching harmful content before it happens, and the other helps staff spot and respond to concerning activity as it happens.

2.1 Filtering - Schools Broadband (Netsweeper)

Every device connected to the school network has its internet access filtered through Netsweeper. Filtering is preventative: it stops content being reached in the first place.

- **Blocks illegal content automatically** - child sexual abuse material and terrorist content lists, supplied by the Internet Watch Foundation and the Home Office/CTIRU. No one at Woodlands, including IT, can switch these off.
- **Blocks other harmful or inappropriate content** - including newly-created sites, using automatic categorisation that doesn't rely on someone adding sites by hand.
- **Applies different rules to different groups** - pupils and staff have different levels of access, and this can be adjusted for a class or year group where needed.
- **Shows the reason** - a block page explains why a site was stopped.
- **Inappropriate searching** - If a member of staff or child searches for something inappropriate and email is sent to the computing lead. Computing lead to talk to staff member/child about the search. Computing lead receives a daily update of the searches that have taken place by staff and children whilst on the school property each day.

What this means for you: filtering does its job without you having to do anything - but it works on categories and lists, not judgement, so it will occasionally block something legitimate you need for a lesson. See section 3 for what to do.

2.2 Monitoring - classroom.cloud (NetSupport)

Pupil laptops and Chromebooks run classroom.cloud. Woodlands' subscription is for live monitoring: monitoring is reactive, so it helps staff notice and respond to something happening in the moment.

- **Live screen viewing** - from your teacher device, you can see what's currently on a pupil's laptop screen, in real time.
- **Remote screen lock** - you can lock an individual pupil's screen instantly if you need to stop what they're doing.

What this means for you: this is the technology equivalent of walking round the room and glancing at screens — except you can do it for every laptop at once, from the front, and step in immediately by locking a screen. It only works if a member of staff is actively watching: Woodlands' current subscription doesn't include automatic keyword alerts or AI activity flags, so there's no background safety net catching things for you.

In the computer room Veyon is used for monitoring of the children. Staff need to be logged in on their own account on the main computer to be able to access this.

3. What this means for you, day to day

- **Make monitoring part of the lesson, not a background app.** Glance at the screen panel regularly during independent or laptop/chromebook-based work — the system only helps if someone's watching.
- **See something concerning? Lock the screen straight away,** then follow the safeguarding process in section 4.
- **Don't work around a blocked site.** If Netsweeper blocks something you genuinely need for a lesson, request it's unblocked rather than using a workaround, personal device or hotspot.
- **Expect occasional over-blocking.** Because the illegal-content lists can't be switched off and categorisation is automatic, useful sites are sometimes caught by mistake - that's the system erring on the side of caution, not a fault.
- **Coverage:** monitoring and filtering apply to school-managed devices on the school network.

4. If you see or suspect something concerning

No matter how small it seems, don't decide for yourself that it isn't worth reporting — pass it on.

Situation	What to do	Who to contact
A pupil may be at risk — something you've seen on a screen, or something a pupil has said or shown you	Follow the child protection policy/online safety policy: record what you saw factually and report it promptly. Record on CPOMS.	Chrissie Coaker Computer lead Record on CPOMS
You're concerned about a colleague's online conduct	Talk to a member of SLT	Dr Victoria Carr Headteacher Alice Morphet DSL

Situation	What to do	Who to contact
A site you need for teaching is blocked	Submit an unblock request — don't try to bypass filtering	Chrissie Coaker Computer Lead or Mark Chadwick, ICT support
Something technical isn't working (filtering or classroom.cloud)	Log a fault with IT support or computer lead	Chrissie Coaker Computer Lead or Mark Chadwick, ICT support

5. Quick FAQ

- **Can pupils tell they're being monitored?** Yes - pupils and parents are told that school devices are filtered and monitored. This is a legal requirement, not something we do quietly. This is covered with the AUP and children can see on the screen when Classroom.Cloud is being used.
- **Does monitoring apply to staff devices too?** Classroom cloud isn't used for teacher and staff accounts. Netsweeper monitors all devices within the school and records all searches from staff and children, when connected to the school network.
- **I need a site unblocked regularly for my subject (e.g. YouTube, a specific tool) - what's the process?** Ask Chrissie Coaker, computer lead and she will email Mark Chadwick who can sort this out.
- **Who can see what I see on Classroom.Cloud?** Only the member of staff running the session sees the live screens; nothing is recorded or sent elsewhere under Woodlands' current subscription.

Key contacts

Designated Safeguarding Lead (DSL): Alice Morphet

Deputy DSL(s): Clare Cotton

IT support / unblock requests: Mark Chadwick

Senior leader responsible for filtering & monitoring: Dr Victoria Carr

This guide summarises the technology Woodlands has in place. It should be read alongside the school's Child Protection & Safeguarding Policy, Staff Code of Conduct / Acceptable Use Policy, and Low-level Concerns Policy.



Filtering and Monitoring — Report to the Governing Body

Prepared by: ICT Support | For: Full Governing Body | September 2026

1. Purpose of this report

This report explains, in plain terms, how Woodlands Primary School filters and monitors pupils' and staff's use of the internet and school devices, and how that provision compares with the Department for Education's (DfE) filtering and monitoring standards, as referenced in Keeping Children Safe in Education (KCSIE) 2026. It sets out clearly for governors what is currently in place and how it supports the school's statutory safeguarding duties.

2. Why this matters

Governing bodies have a statutory duty under KCSIE 2026 to ensure the school has appropriate filtering and monitoring systems in place, and to review their effectiveness at least once every academic year.

Filtering is preventative: it stops pupils and staff reaching illegal, harmful or inappropriate content. Monitoring is reactive: it picks up concerning activity on school devices so staff can step in and support a pupil. The DfE sets out four standards schools should meet; section 4 below sets out how Woodlands' current provision maps against each one.

3. What Woodlands has in place

Woodlands uses two complementary systems: Schools Broadband (Netsweeper) filters what pupils and staff can reach on the internet, and classroom.cloud (NetSupport) monitors what is happening on pupil laptops and Chromebooks in real time. In addition to this in the computer room on the junior site Veyon is used for monitoring of the children. Staff need to be logged in on their own account on the main computer to be able to access this.

Used together, they are designed to meet both the "filtering" and "monitoring" elements the DfE and KCSIE 2026 require schools to have in place.

3.1 Filtering - Schools Broadband (Talk Straight), powered by Netsweeper

All internet access on the school's network is filtered through Netsweeper, supplied as part of the Schools Broadband service. It provides:

- Statutory illegal-content blocking - Schools Broadband has been a member of the Internet Watch Foundation (IWF) since 2013. Netsweeper applies the IWF's child abuse image content block list and image hash list, and the Home Office/Counter-Terrorism Internet Referral Unit (CTIRU) list of unlawful terrorist content. Neither list can be switched off, edited or bypassed by the school.
- Automatic categorisation of new sites - an AI-based categorisation engine identifies and blocks newly-created harmful websites as they appear, without needing to be added manually.
- Age- and role-appropriate profiles - different filtering policies can be applied by username, group or IP range, so pupils and staff have different, appropriate levels of access.
- Local control - the school can add or remove specific sites or categories itself, for example to block extra content or unblock something needed for a lesson.

- Transparency - a block page with a stated reason is shown whenever a site is blocked.
- Basic monitoring and reporting - Netsweeper logs and reports on internet use across the network, viewable through a management portal. This is the network-level "basic monitoring" already in place at Woodlands.
- Inappropriate searching - If a member of staff or child searches for something inappropriate and email is sent to the computing lead. Computing lead to talk to staff member/child about the search. Computing lead receives a daily update of the searches that have taken place by staff and children whilst on the school property each day.

3.2 Monitoring - classroom.cloud by NetSupport

Pupil laptops also run classroom.cloud. Woodlands' subscription is for live monitoring only, and provides:

- Live screen viewing - staff can see, in real time, what is displayed on a pupil's laptop screen during lessons.
- Remote screen lock - staff can lock a pupil's screen instantly if they need to stop or pause what the pupil is doing.

This gives staff a real-time equivalent of walking around a classroom and looking at screens, across every laptop in the session, with the ability to step in immediately by locking a screen. Woodlands' current subscription does not include classroom.cloud's automated keyword/phrase alerting, AI-activity tracking or case-logging features.

Together, these two systems support the DfE's filtering and monitoring standards referenced in KCSIE 2026: Netsweeper delivers the statutory illegal-content blocklists and general web filtering required under the "filtering" element, while classroom.cloud provides live, teacher-led visibility of pupil laptop screens, which supports the "monitoring" element expected alongside filtering.

4. How this maps against the DfE's four standards

This is a summary based on the technology in place. Some elements depend on local school practice (who is named as responsible, when reviews take place, what policies say) rather than the systems themselves — these are flagged for the school to confirm to governors.

DfE standard	What it requires	Woodlands' current position
1. Roles and responsibilities	A named senior leader and a named governor should be responsible, with clear roles for the DSL, IT support and staff.	Victoria Carr, Headteacher Kelly Hutton Safeguarding governor
2. Annual review	Provision should be reviewed at least once every academic year by the SLT, DSL and IT support, with the responsible governor involved, and a record kept.	Reviewed September 2026 by ICT support
3. Filtering blocks harmful content	The filtering provider must be an Internet Watch Foundation (IWF) member, apply the Home Office/CTIRU terrorism block list, and this cannot be switched off. It should cover	Well supported by the technology: Schools Broadband/Netsweeper has been an IWF member since 2013 and applies the IWF child abuse image list

DfE standard	What it requires	Woodlands' current position
	all devices, users, sites and any guest or BYOD access.	and the Home Office terrorism list; these cannot be disabled locally. Staff own devices are not supported by this and should not be allowed on the school network.
4. Effective monitoring	A monitoring plan should combine technical and in-person monitoring, produce at least weekly reports plus immediate alerts for high-risk incidents, and set out how staff respond to and record concerns. Users should be told monitoring takes place.	Classroom.Cloud gives staff live visibility of pupil screens and the ability to lock a screen if needed — a technology-supported form of the in-person/device monitoring the standard describes. As this is live, teacher-led monitoring rather than automated keyword-based alerting, it depends on a member of staff being actively watching. As the AUP states, children should not be left unsupervised with school computing devices or use staff devices and logins.

These are revised with children at the start of each term during the first computing lesson.

Key Stage 1



Key Stage 2

