

Online Safety Policy

Author of Policy	Catherine Jermyn, DSL
Policy Approved by	Local Academy Council
Date	July 2026
Review Date	July 2027



1 Policy and leadership

1.1 Scope of the Online Safety Policy

This Online Safety Policy sets out how Pendle Primary Academy 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, children, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Pendle Primary Academy will respond in line with this policy and related procedures, including the school's Child Protection and Safeguarding Policy; Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy and other related policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that takes place out of school.

1.2 Policy development, monitoring and review

This Online Safety Policy has been developed by the Designated Safeguarding Lead (DSL) in consultation with the Principal, Safeguarding Governor and Pendle Education Trust (PET) DSL Cluster and Online Safety Group.

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

1.3 Schedule for development, monitoring and review

This Online Safety Policy was approved by the Local Academy Council on:	15 th July 2026
The implementation of this Online Safety Policy will be monitored by:	Catherine Jermyn (DSL), School Safeguarding Governor and PET DSL Cluster and Online Safety Group
Monitoring will take place at regular intervals:	Termly in Online Safety Group meetings with a full review annually in the Spring term.
The Online Safety Group will receive a verbal update on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	Termly in Online Safety Group meetings.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next review will take place no later than:	July 2027



1.4 Process for monitoring the impact of the Online Safety Policy

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

- Logs of reported incidents from CPOMS
- Filtering and monitoring records
- Internal network activity monitoring data
- Surveys/questionnaires of children, parents/carers, staff

1.5 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.

1.5.1 Principal and Senior Leadership Team (SLT)

The Principal and SLT set the culture and ensure that systems are effective. In line with Keeping Children Safe in Education (KCSiE), the Designated Safeguarding Lead (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 (Principal plus at least one senior leader).
- Ensure that the DSL, PET IT Team and relevant colleagues are trained and able to fulfil their roles.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with the Local Academy Council, PET Trust Board, the DSL and PET IT Team on filtering and monitoring.

1.5.2 Governors – Local Academy Council (LAC)

LAC approve the Online Safety Policy and challenge its effectiveness, in line with KCSiE expectations.

LAC will nominate a Safeguarding Governor who will:

- Meet at least termly with the DSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and PET IT Team, in line with DfE standards.



- Report to the LAC.
- Undertake basic cyber security awareness training and support school cyber security oversight.

1.5.3 Designated Safety Lead (DSL)

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

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Co-ordinate 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 incident patterns and filtering/monitoring information, confirming at least annual checks.
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review using 360 safe).
- Ensure appropriate support for children with SEND.
- Attend Online Safety Group meetings as part of the PET DSL Cluster.
- Lead development and review of online safety documentation.
- Co-ordinate awareness, staff confidence and reporting readiness through appropriate training.
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with PET IT Team and school wellbeing/mental health/pastoral support staff.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

1.5.4 Curriculum Leadership Team

Curriculum Leadership Team (which comprises of Curriculum Design Leader (also the DSL), Curriculum Delivery Leader and Curriculum Effectiveness Leader) will work with the DSL to develop a planned and online safety education programme through appropriate channels, e.g. Computing, PSHE and other curriculum areas; assemblies; wellbeing provision and national initiatives e.g. Safer Internet Day. The school's planned online safety curriculum is based on the [Education for a Connected World Framework](#) and [ProjectEVOLVE](#) resources.

1.5.5 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, Child Protection and Safeguarding Policy, PET Technical Security Policy and read, understand and commit to following the PET Staff IT AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise child 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.

1.5.6 PET IT Team

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

The PET IT Team 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 Principal and/or DSL.
- Monitor systems for misuse and report concerns promptly to the Principal and/or DSL.
- Follow the PET Technical Security Policy and maintain adherence to the school's Online Safety Policy and keep technical knowledge current.

1.5.7 Children

Children will:

- Follow the Children's SHINE Charter and #BESAFE rules.
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly (where permitted): protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.



1.5.8 Parents and carers

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

The school will:

- Publish the Online Safety Policy on the school website and share the Children's Shine Charter and #BESAFE rules when a child starts school.
- Provide guidance on the responsible use of online technologies via the school newsletter and school website.
- Gain consent for digital services and publishing of images where required.
- Share online safety updates through meetings, newsletters, online channels and campaigns.

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

- Reinforcing the online safety messages provided to children at home and upholding the principles of online safety in the SHINE charters.
- Ensuring their children do not bring personal devices, including mobile phones and smart watches to school under any circumstances.

1.5.9 Community users

Community users accessing school systems will sign a PET Visitor IT AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

1.6 Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. The PET DSL Cluster and Online Safety Group is made up of:

- Senior Leaders / DSL from all the PET schools.
- Online Safety Leads of all the PET schools (where this leader is not the DSL).
- PET IT Technical staff.

Minutes of DSL Cluster / Online Safety Group meetings are sent to the PET Safeguarding Trustee for scrutiny after each meeting.

The Online Safety Group supports the DSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.



- Gather feedback from children, staff and parents/carers and turn this into improvement actions.
- Promote child voice, peer support and awareness activity.
- Track and evidence improvement actions (e.g. Use of 360 Safe).

2 Policy

2.1 Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside the Child Protection and Safeguarding Policy; Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy; Data Protection and other related policies.

What the Online Safety 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 children's digital competence and critical understanding.

Implementation, monitoring and review of the Online Safety Policy:

- Developed through the Online Safety Group and reviewed at least annually, and sooner if risks/technology change.
- Monitored by the DSL, Safeguarding governor and Online Safety Group using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 Safe, ProjectEVOLVE).
- Findings inform improvement planning and staff training priorities.

Communication and accessibility of the Online Safety Policy:

- Shared at staff induction and reinforced through training and staff updates.
- Communicated to children and parents/carers through AUAs and awareness activity.
- Policy is published on the school website.

2.2 Acceptable use

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

The PET Staff ICT Acceptable Use Agreement (AUA) is shared with all staff at induction and at the start of every academic year thereafter. Staff members must confirm that they have read, understood and will follow the AUA at induction and then annually at the start of every academic year.



The PET Visitor AUA (which is signed by any visitor using school devices, as well as volunteers, students (including work experience placements), supply staff, agency staff, contractors, community users and parents) is shared with visitors at the point at which they require access to school systems/devices or induction in the case of supply staff / work experience placements etc. that are working in school over a longer period.

The AUA for children and parents/carers is part of the SHINE charters that are shared with children and parents/carers when a child starts school and by asking parents/carers to acknowledge these by signing the document as means of agreeing to the principles therein. The SHINE charters are on the school website, in the school's welcome booklet and on display around the school building. They are also shared periodically in the school newsletter.



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



User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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>					X



User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. <i>(Informed by the school's filtering practices and/or AUAs)</i>				X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	



When undertaken for non-educational purposes and using school devices / systems (unless otherwise stated)	Staff and other adults				Children	
	Not allowed	Allowed	Allowed at certain times/places	Allowed for selected staff	Not allowed	Allowed
Online gaming and in-game chat/voice <i>e.g. Roblox, Fortnite, Minecraft</i>	X				X	
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)			X		X	
Cloud storage and file sharing <i>e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents</i>	X				X	
Social media and user-generated platforms <i>e.g. TikTok, Instagram, Snapchat, X, Reddit, and other age-restricted services</i>	X				X	
Messaging, chat and voice <i>e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts</i>	X				X	
Legal streaming entertainment/media (video, music, podcasts) <i>e.g. Netflix, Disney+, Spotify</i>			X		X	
Video platforms and livestreaming <i>e.g. YouTube, Twitch, TikTok LIVE, Instagram Live</i>	X				X	
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds)		X			X	
Use of personal mobile phones in school			X		X	
Taking photos/video/audio on personal devices (including sharing, location data and consent)			X		X	
Other personal devices <i>e.g., tablets, handheld consoles, VR headsets, wearables</i>			X		X	
Personal email accounts on site or on the school network/Wi-Fi <i>e.g., Gmail, Outlook.com</i>			X		X	
School email used for personal communication	X				X	
Unapproved AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)	X				X	



2.3 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 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.

2.3.1 Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including children, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the Child Protection and Safeguarding, Whistleblowing, Managing Allegations Against Staff and Complaints policies.
- Multiple reporting options are available, such as speaking with the DSL, online or anonymous reporting tools (via PPA Stars website), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

2.3.2 Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL and other senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
 - Child sexual abuse material (CSAM)
 - Non-consensual or self-generated images
 - Grooming, exploitation, or sexual harassment
 - Terrorism or extremism
 - Hate crime, fraud, extortion, stalking



- Cyber offences under the Computer Misuse Act
 - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

2.3.3 Recording and Monitoring

The school will:

- Maintain a secure and confidential record of all incidents (using CPOMS where the incident involves a child and CPOMS StaffSafe where the incident involves a member of staff), including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
 - The Online Safety Group
 - Senior leaders
 - Local Academy Council via Safeguarding Governor
 - Staff, where appropriate
 - Children, where appropriate
 - Parents/carers through general communications
 - Local safeguarding partners, where relevant

2.3.4 External Support and Escalation

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

- Lancashire Children's Social Care (CSC)
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership (e.g., harmful sexual behaviour support)
- UK Safer Internet Centre's Professionals Online Safety Helpline
- Reporting Harmful Content service

2.3.5 School actions

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



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 child / staff member to determine what happened.
Update parents/carers on incident as applicable.

Ensure the wellbeing of those involved is addressed.
Ensure Incident Log 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.

*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.

2.3.6 Responding to incidents involving children's actions

Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to DSL or Principal	Refer to Police / CSC	Refer to PET IT Team for support / action	Inform parents/carers	Remove device / Wi-Fi / network access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.			X	X	X	X	X	X
Unauthorised access to the school network , including using another person's account or sharing usernames/passwords.		X	X			X	X	X
Damaging, corrupting or deleting another user's data.		X				X	X	X
Sending offensive, harassing or bullying emails, texts or messages.			X			X		X
Unauthorised downloading/uploading , file sharing or distribution of files.		X			X			X
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).		X			X	X	X	X
Failing to report accidental access to offensive or pornographic material			X		X	X		
Deliberately accessing offensive or pornographic material (or attempting to)			X		X	X	X	X
Sharing or receiving content that breaches copyright or data protection law.		X			X	X		
Unauthorised use of devices , including taking photos/videos or audio recordings.		X	X			X	X	X
Unauthorised use of online services (apps, websites or platforms).		X			X			X
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.			X			X	X	X
Repeated breaches of these rules following previous warnings or sanctions.			X			X	X	X



2.3.7 Responding to incidents involving staff actions

Incidents	Refer to line manager	Refer to Principal	Refer to PET / HR	Refer to Police and/or LADO	Refer to PET IT Team for support / action	Issue a warning / management instruction	Further action, in line with disciplinary procedures
Accessing illegal material (or attempting to), as defined in the earlier “Unsuitable/Inappropriate Activities” section.		X	X	X	X		X
Breaching data protection or cyber-security requirements , including network security rules.		X	X		X	X	X
Accessing offensive or pornographic material (or attempting to).		X	X	X	X		X
Damaging systems or data , including corrupting/deleting others’ data or deliberately damaging hardware/software.		X	X		X	X	X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).		X	X		X	X	X
Unauthorised downloading, uploading or file sharing .		X	X		X	X	X
Breaching copyright, licensing or intellectual property , including misuse of AI systems.		X	X		X	X	X
Unauthorised account/network access , including sharing passwords, using another person’s account, or allowing others access.		X	X		X	X	X
Sending offensive, harassing or bullying emails, texts or messages.		X	X	X	X	X	X
Use of personal email/social media/messaging to communicate with children or parents/carers.		X	X			X	X
Inappropriate personal use of school technology , including personal email and social media use during work time/using school systems.	X	X	X			X	X
Mishandling personal data , including storing, displaying or transferring it insecurely.	X					X	
Any action that undermines professional conduct or a staff member’s professional standing.	X					X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X				X	
Failing to report incidents , whether accidental or deliberate.	X	X				X	
Repeated breaches following previous warnings or sanctions.		X	X				X



3 Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements and by updating procedures where needed. Safeguarding of children and staff remains central to our approach.

3.1 AI Policy Statements

The school will:

- Support appropriate use of AI to enhance learning and teaching; improve outcomes; streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including KCSiE and UK GDPR.
- Provide training and guidance for staff and the LAC on the benefits, risks and safe use of AI and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping children to understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

3.2 Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools other than those secured within the school's Google Workspace for Education or PET Microsoft 365 account. Where other AI tools are 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 by only using tools approved by PET IT Team.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff must only use school-provided AI accounts 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 by the PET IT Team.



3.3 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.
- 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 children, including ensuring children's work is not used to train AI systems without appropriate consent.

3.4 Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the DSL.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

The PET IT Team will:

- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using an appropriate risk assessment matrices.

3.5 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 children in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

3.6 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 disciplinary action being taken, as set out in the PET Managing Discipline procedure.



4 Education

4.1 Online Safety Curriculum

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 children, aligned to nationally recognised guidance and frameworks (including [DfE "Teaching Online Safety in Schools"](#), [UKCIS "Education for a Connected World"](#), and resources such as [SWGfL ProjectEVOLVE](#)). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including PSHE and Computing), with assessment and clear intended outcomes.

The curriculum develops children's ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks
- understand consent and abuse online at an age-appropriate level, supported by supported, 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 and intellectual property, including when using online material and AI tools
- understand and follow Children's SHINE Charter and #BESAFE rules, and act within moral and legal boundaries (including an age-appropriate awareness of the [Computer Misuse Act 1990](#)).

Where internet use is planned, children are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise closely and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Child's voice is actively used to strengthen the school's approach through feedback, child representation (e.g. Academy ambassadors) and opportunities such as community-facing online safety activities.

4.2 Staff

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.



- All staff will receive online safety training and understand their responsibilities under this policy. Training will include: annual safeguarding training for all staff; an annual online safety update through the school's CPD offer for teaching and learning staff; biennial Online Safety accreditation for teaching and learning staff; regular updates in response to new risks/incidents through email, staff briefings etc.
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources, including completion of biennial Online Safety accreditation for teaching and learning staff.
- 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 to individuals as required.

4.3 LAC (Governors)

Governors should take part in online safety training and awareness activity. This is particularly important for the Safeguarding governor.

Training and updates may be provided through:

- Attendance at training offered by the Local Authority and PET.
- 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 to review key themes, incidents and current priorities and/or the DSL providing overview of these at a LAC meeting.

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

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



4.4 Families and external stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of children. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

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

4.4.1 Working with parents and carers

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

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carers workshops, information events, or drop-ins focused on online safety.
- Involving children in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. [UK Safer Internet Centre](#), [Internet Matters](#), [Childnet](#), [SWGfL](#)).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.

4.5 Wider community and agencies

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

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.



- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

5 Technical Safeguarding

The school recognises that effective filtering, monitoring, technical security, cybersecurity 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.

5.1 Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., DfE Technical Standards, KCSiE) and best practice guidance.

The school and PET IT Team 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 children 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.

5.1.1 Oversight and review

- The PET IT Team, DSL and governors have clear roles and responsibilities.
- Filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g. using [Testfiltering](#)).
- Log reports provide actionable information for safeguarding decisions.
- No system is relied upon in isolation; reporting routes and professional judgement remain central.



5.2 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 and PET IT Team ensures that:

- Access to systems and data is controlled through appropriate authentication and permissions.
- Devices, networks and systems are protected through secure configuration, patching and malware protection.
- Backups and recovery arrangements are in place to reduce the impact of system failure or attack.
- Incidents and weaknesses are reported, recorded and used to inform improvement
- Responsibilities for technical security are clearly defined and supported by appropriate expertise.
- Systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

5.3 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 and PET IT Team ensures that:

- A cyber security approach is in place to prevent, detect, respond to and recover from cyber threats.
- Senior leaders and governors understand cyber risks and receive appropriate assurance.
- Staff and children 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.

5.4 Data Protection

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

The school and PET IT Team 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.

5.5 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.

6 Technology Practice

6.1 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, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice and education.

6.2 Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects the KCSiE 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, children 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.

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

The school does not allow children to bring personal digital devices into school under any circumstances, this includes the wearing of smart watches. *See also: Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy.*

The school allows:

	School Devices		Personal Devices		
	School owned for individual use	School owned for multiple users	'Child' owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes			
Internet only				Yes – using Guest Wifi	Yes – using Guest Wifi
No network access					

6.3 Digital Content

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

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 children are trained/educated to understand their responsibilities when creating or sharing digital content.
- Personal data and images are handled securely and lawfully.
- Policy and practice are reviewed in the light of emerging technologies and risks.



6.4 Public Online Communications

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

The school ensures that:

- Public online communications are appropriate, accurate and well-managed.
- Public communications from or regarding the school are monitored and addressed where appropriate.
- Published content complies with safeguarding, data protection and statutory requirements.
- Where children's work, images or videos are published by the school, their identities are protected, and full names are not published.
- To reduce the risk of illegal manipulation of publicly available images of staff and children, the school has procedures in place to control how those images are shared online, following [guidance from UKSIC](#).
- Online safety information is shared with parents, carers and the wider community.
- Clear processes exist for managing school online accounts.
- Staff understand expectations around professional conduct and online behaviour.

6.5 Review

Technology practice is reviewed regularly to reflect:

- Changes in technology and online behaviour.
- Emerging safeguarding risks.
- Feedback from staff, children and parents.
- National guidance and statutory expectations.

7 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, children and parents/carers. The effectiveness and of the curriculum and children's outcomes are evaluated by the curriculum effective leader. 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

8 See also / related policies, procedures and documents

- SHINE Charters
- Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy
- Child-on-Child Abuse Procedure
- Prevent Duty Risk Assessment and Procedure
- Curriculum Policy
- Remote Learning Plan
- Curriculum Policy
- Curriculum Maps
- Curriculum Progression documents for Computing and PSHE
- PET Social Media Policy
- PET Technical Security Policy
- PET Staff ICT Acceptable Use Agreement
- PET Visitor ICT Acceptable Use Agreement
- PET Staff Code of Conduct

