



THE ELMS

Online Safety Policy	
Version	2026.1.1
Effective from	Sept 2026
Extent of Policy	The Elms School
Policy Owner	Designated Safeguarding Lead / Online Safety Lead
Authorised by	Chair of Governors
Review by	September 2027
Frequency of Review	Annual
Circulation	Governors All Employees Parents by request
Publication	Website Teaching Staff Handbook

Table of Contents

Scope of the Online Safety Policy	3
Policy development, monitoring and review	3
Schedule for approval, monitoring and review	3
Policy and leadership.....	4
Responsibilities	4
Online Safety Group	8
Policy.....	9
Online Safety Policy.....	9
Acceptable use	10
Reporting and responding	15
Responding to Learner Actions.....	17
Responding to Staff Actions.....	18
Use of Artificial Intelligence (AI)	18
Education.....	21
Online Safety Education Programme.....	21
Staff.....	22
Governors	22
External Stakeholders	23
Working with Parents and Carers.....	23
Wider Community and Agencies.....	24
Technology.....	24
Filtering and Monitoring.....	25
Technical Security.....	26
Cyber Security	27
Data Protection.....	27
Technology Practice	28
Device Management.....	28
Digital Content.....	29
Public Online Communications.....	29
Outcomes.....	30

Scope of the Online Safety Policy

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

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, The Elms School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school. Where there is any conflict between this policy and the Safeguarding/Child Protection Policy, the safeguarding policy and statutory guidance take precedence.

Policy development, monitoring and review

This policy has been developed by the **Welfare Committee** drawing on the expertise and responsibilities across the school. Membership includes:

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

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

Schedule for approval, monitoring and review

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

Monitored by: DSL & OSL

Monitoring frequency: During DSL & OSL bi-weekly Meetings

Reporting to the Governing Body: Termly – through Welfare Committee meetings, IT Reports & Termly meetings with Welfare Governor, DSL & OSL.

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

Escalation following serious incidents: the school will inform relevant external agencies as appropriate.

Monitoring the impact of the policy

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

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

Policy and leadership

Responsibilities

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

Headmaster 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 (Headmaster plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.

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

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and OSL, in line with KCSIE and DfE Filtering and Monitoring standards.
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Participate in the Online Safety Group.

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

Designated Safeguarding Lead (DSL)

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

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT Manager and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- The DSL and the IT Manager lead the review of the effectiveness of filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

Online Safety Lead (OSL)

The OSL will:

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

Curriculum Leads

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

Teaching and Support Staff

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

Staff will:

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

IT Manager & external providers

The IT Manager and external providers support leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT Manager, with the support of any external providers provider will:

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

Learners

Learners will:

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

Parents and carers

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

The school will:

- Publish the Online Safety Policy and share the learner AUA
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

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

Community users

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

Online Safety Group

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

Membership

- DSL, OSL, Senior Leader(s)

- Online Safety Governor
- Staff representatives (teaching/support)
- Learner representative(s)
- Parent/carer representative(s)
- Community/external partner (where relevant)

Core responsibilities

The group supports the DSL/OSL to:

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

Governance and impact

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

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.

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

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually, and sooner if risks/technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity.
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

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

Acceptable use

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

Reinforcement

- staff induction
- on-screen reminders (e.g. splash screens)
- curriculum and awareness sessions
- communications with parents/carers
- peer support / learner-led activity
- ICT Lessons

Acceptable/Unacceptable Actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • <i>Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).</i>					X
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	- Disabling, impairing or disrupting network/services (e.g., denial of service) - Using penetration-testing tools without explicit permission					
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (e.g. Roblox, Fortnite, Minecraft)	X				X			
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)		X			X			
Cloud storage and file sharing (e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents)		X						X
Social media and user-generated platforms (e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services		X			X			
Messaging, chat and voice (e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)		X			X			
Streaming entertainment/media (video, music, podcasts) e.g. Netflix, Disney+, Spotify		X			X			

Video platforms and livestreaming (e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)		X						X
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds).		X			X			(Provision made for boarders)
Taking photos/video/audio on devices (including sharing, location data and consent)		X						X
Other personal devices (e.g., tablets, handheld consoles, VR headsets, wearables)		X			X			Provision for boarders
Personal email accounts on site or on the school network/Wi-Fi (e.g., Gmail, Outlook.com)		X				X		
School email used for personal communication (non-work/non-learning)	X					X		
Unapproved AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)	X				X			

Reporting and responding

Introduction

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

The school recognises national findings, including the *Ofsted Review of Sexual Abuse in Schools and Colleges (2021)*, which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the OSL or DSL, online or anonymous reporting tools (e.g., Confide), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies & posters.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated promptly through safeguarding procedures. Examples include (but are not limited to):

- Child sexual abuse material (CSAM)
- Non-consensual intimate images or self-generated intimate 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 where appropriate and lawful, using a safe, controlled and documented process involving authorised senior staff and, where appropriate, a designated review device. Staff must not undertake their own investigation of suspected criminal activity and will follow safeguarding, data protection and external-agency advice where applicable.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns will receive reassurance and appropriate support, and, where appropriate and lawful, feedback on the outcome.

Recording and Monitoring

The school will:

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

External Support and Escalation

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

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

The actions indicated below are potential responses and are not intended to prescribe an automatic response to every incident. The school will consider the nature, severity, intent, impact and context of each incident, including safeguarding concerns and the individual circumstances of the learner or staff member. Safeguarding concerns will be managed in accordance with the Safeguarding/Child Protection Policy and relevant statutory guidance.

Responding to Learner Actions

Incident	Staff/DSL response	Technical response	Parent/carers	Behavioural response	External referral
Accidental inappropriate access	Appropriate staff/DSL as required	Check/filter if necessary	Where appropriate	Education/support	Normally no
Deliberate inappropriate access	DSL/SLT as appropriate	Restrict/check as proportionate	Where appropriate	Behaviour process	Where required
Suspected illegal material	Safeguarding procedure	Preserve evidence / technical support	Only where appropriate and safe	As appropriate	DSL determines appropriate referral
Cyber/security misuse	IT + appropriate senior staff	Secure account/system	Where appropriate	Behaviour process	Where required
Bullying/harassment	DSL/behaviour process	Preserve/report content	Where appropriate	Behaviour/restorative response	Where required
Repeated breaches	SLT/DSL	Proportionate restrictions	Where appropriate	Behaviour process	Where required

Responding to Staff Actions

Incident	Management route	Safeguarding	DPO/IT	External/disciplinary
Routine policy breach	Line manager	—	As required	Management action
Data breach	Line manager/DPO	If safeguarding issue	DPO/IT	ICO where required
Cyber-security breach	Line manager/IT	If safeguarding issue	IT/DPO	As required
Inappropriate communication	Line manager/DSL	DSL if learner involved	As required	Management/disciplinary
Professional boundary concern	DSL/Headmaster	Safeguarding procedure	As required	LADO/police where threshold met
AI / Image generation misuse	DSL/Headmaster	Managing Allegations procedure	As required	LADO/police/other agency as appropriate
Serious safeguarding allegation	DSL/Headmaster	Managing Allegations procedure	As required	LADO/police/other agency as appropriate
Deliberate concealment	Line manager/Headmaster	DSL if relevant	DPO/IT if relevant	Disciplinary process

Use of Artificial Intelligence (AI)

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

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by

updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

Policy statements

The school will:

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

Safe use, data protection and security

The school will:

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

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to **IT Manager & DPO**
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices in Appendix C7.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback). Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

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

Education

Online Safety Education Programme

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

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks. 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), with assessment and clear intended outcomes.

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 and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the [Computer Misuse Act 1990](#)).

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant – and are expected to use monitoring software (e.g. Impero). Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback and learner representation (e.g. on an Online Safety Group).

Staff

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

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include (select/delete as appropriate):
- 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.
- An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (KCSIE 2026)
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources 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 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, MAT or other relevant organisations.
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

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

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

External Stakeholders

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

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

Working with Parents and Carers

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

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

- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources.
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.

Wider Community and Agencies

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

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- 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.

Technology

Purpose

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

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., [DfE Technical Standards](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The 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 monitoring plan will include at least weekly review of monitoring reports to identify incidents, patterns and emerging safeguarding concerns, with high-risk safeguarding, malicious or technical incidents escalated immediately to the appropriate staff in accordance with the School's safeguarding and incident-response procedures.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities

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

Technical Security

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

The school ensures that:

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

Cyber Security

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

The school ensures that:

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

Data Protection

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

The school ensures that:

- Its systems and suppliers/vendors are, at a minimum, compliant with the cyber essentials standards. Vendors that hold pupil and staff information are expected to hold Cyber Essentials Plus or ISO 27001 certification.
- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements

- data protection is embedded across safeguarding, teaching, learning and administration
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

Review

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

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

Technology Practice

Purpose

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

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

Device Management

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

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use

- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- In line with the [DfE statutory guidance](#), the school prohibits for learners the use of mobile phones and other personal devices throughout the school day, including during lessons, or between lessons, breaktimes and lunchtime. Allowance is made for boarders, who can use their devices for calling their parents only, this is within specific calling area's in the boarding house and phones must be stored in the designated space.

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

Digital Content

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

The school ensures that:

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

Public Online Communications

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

[manipulation and abuse](#)

The school ensures that:

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

Review

Technology practice is reviewed regularly to reflect:

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

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

Appendix A1 - Acceptable Use Agreement Template

Acceptable Use Agreement

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

Keeping Safe Online

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

Using Computers and the Internet Sensibly

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

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.

- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules?

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

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

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

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

Name of Learner:.....Class:.....

Signed:Date:

Parent/Carer Countersignature

Name of Parent:.....Class:.....

Signed:Date:

Appendix A2 - Staff Acceptable Use Agreement Template

School Policy

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

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school

- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. If I use my personal equipment to record these images, these images will be uploaded to the schools media facilities and then deleted within 7 days from my device.
- I will only use social networking sites in the school in accordance with school policies.
- I will not engage with pupils or former pupil on Social Media whilst they are under 16 years old.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:

- will only use AI technologies approved by the school
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up-to-date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy).
Where digital personal data is transferred outside the secure local network, it must

be encrypted. Paper based documents containing personal data must be held in lockable storage.

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

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

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content

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

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

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

Staff Name:

Signed:

Date:

Appendix A3 - Online Safety Policy Statement

At The Elms School, we want every user to be safe, confident and supported when using technology - whether learning in school, at home, or in the wider community. Online safety is part of safeguarding and wellbeing. It is not “just an IT issue”: it is about people, relationships, behaviour, learning, and protection.

Our online safety strategy is built around four outcomes-focused areas that strengthen day-to-day practice:

- Leadership and policy that make expectations clear
- Education that builds skills, resilience and positive behaviour
- Technology that protects users and supports safe learning
- Impact review that proves what’s working and what we will improve

Leadership and policy: clarity, consistency and accountability

- When leadership is strong, online safety becomes part of “how we do things here”—not a one-off initiative.

Clear responsibilities

- We make sure roles are defined and understood across senior leaders, the Designated Safety Lead, an Online Safety Lead, governors and technical service providers. This ensures safeguarding decisions and technical safeguards work together.
- What this improves: decisions are quicker, concerns are escalated correctly, and actions don’t get “lost” between teams.
- Benefit for users: children and adults get safer, more consistent support.

A joined-up Online Safety Group

- We involve the right voices—leaders, staff, governors, and (where appropriate) learners—to keep online safety responsive to real experiences and emerging risks.
- What this improves: shared ownership and a whole-school approach.
- Benefit for users: safer practice is reinforced across school and home.

A policy that is understood and used

- Our online safety policy is aligned with safeguarding expectations and linked to related policies so that staff and families can see one clear, consistent approach.
- What this improves: fewer grey areas and more confident decision-making.
- Benefit for users: clear boundaries and predictable responses.

Acceptable use expectations that protect everyone

- We set out simple, age-appropriate expectations for learners and clear professional expectations for staff, so everyone understands what safe and respectful use looks like.
- What this improves: behaviour, consistency, and fairness.
- Benefit for users: safer online spaces and fewer harmful incidents.

Reporting and responding that leads to action

- We promote a culture where people feel able to speak up, and we respond consistently, recording concerns, acting promptly, and learning from patterns and new risks.
- What this improves: early identification and effective safeguarding intervention.
- Benefit for users: children get help sooner; everyone feels listened to and protected.

Education: confident learners and informed adults

- We teach online safety to build knowledge, skills, attitudes and resilience—so learners can enjoy the benefits of technology while managing risks.

Planned learning for learners

- Online safety education is progressive, inclusive and revisited regularly.
- What this improves: safer choices, healthier online behaviour, and confident help-seeking.
- Benefit for users: learners become better prepared for real-life online challenges.

Staff training that supports safeguarding practice

- All staff receive induction and ongoing updates so they can spot concerns, respond appropriately, and model safe practice. Key roles receive enhanced training to lead and make informed decisions.
- What this improves: confidence and consistency across the workforce.
- Benefit for users: concerns are handled calmly, correctly and promptly.

Governors trained to provide challenge and support

- Governors understand their duties and can ask the right questions about policy, training, curriculum, filtering/monitoring, and cyber security.
- What this improves: accountability and sustained improvement.
- Benefit for users: online safety stays a priority over time, not just after incidents.

Strong partnerships with families and agencies

- We communicate practical guidance to families and work with relevant partners. We also share effective practice beyond our school where it supports safer communities.
- What this improves: joined-up messages and earlier support.
- Benefit for users: children experience consistent expectations across school and home.

Technology: protection that enables learning

- We use proportionate technical controls to reduce exposure to harm while supporting teaching and learning.

Effective filtering

- Filtering reduces the risk of access to harmful and illegal content and is reviewed to ensure it stays fit for purpose.
- Benefit for users: safer browsing and research.

Safeguarding-led monitoring

- Monitoring helps identify concerns early and supports timely intervention, handled with appropriate governance and data protection.
- Benefit for users: timely intervention when risk is emerging.

Secure systems and cyber resilience

- We protect networks, devices and accounts, and we prepare for threats like phishing and ransomware—so learning is not disrupted and users are protected.
- Benefit for users: safer services, fewer incidents, faster recovery.

Data protection that builds trust

- We handle personal and sensitive information carefully and lawfully, with clear processes and accountability.
- Benefit for users: privacy is respected and risks from misuse are reduced.

Safe day-to-day practice

- We manage devices consistently (including expectations around personal devices where relevant), apply safeguarding and consent to digital content, and communicate responsibly through our public channels.
- Benefit for users: fewer avoidable mistakes and a safer, more responsible digital culture.

Impact: proving what works and improving what doesn't

- We regularly review how well our policies and practice are working, what the evidence tells us, and what we will improve next. This keeps our approach current, targeted and effective.

How to raise a concern or get help

If something online worries you, we want to know.

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

Our commitment

We will keep strengthening leadership, education, technology and impact review so that technology at The Elms School used safely, respectfully and positively—and so our community can be confident that online safeguarding is robust, consistent, and always improving.

Appendix A4 – Computer Misuse and Cyber Choices Policy

Purpose

The purpose of this policy is to set out the school's approach to preventing, identifying and responding to computer misuse and potential cybercrime involving learners.

Computer misuse is recognised as a safeguarding issue and this policy supports the school's wider safeguarding, Online Safety, Filtering and Monitoring, Technical Security and Cyber Security arrangements.

This policy aligns with [Keeping Children Safe in Education](#) (KCSIE), [the Computer Misuse Act 1990](#), [National Crime Agency \(NCA\) Cyber Choices](#) guidance, and [DfE Filtering and Monitoring and Technical Standards](#).

Scope

This policy applies to:

- All learners, staff, volunteers and governors
- Behaviour occurring within and outside school where it impacts the school community

Policy Statement

The school will ensure that:

- Learners understand that some online activity is illegal
- Acceptable Use Agreements clearly outline legal expectations and consequences
- Computer misuse is treated as a safeguarding concern in the first instance
- Staff understand emerging cyber risks and referral routes
- Concerns are referred immediately to the Designated Safeguarding Lead (DSL)
- Appropriate external advice or referral is sought where required

Prevention and Education

The school will ensure that:

- Learners are taught about the Computer Misuse Act 1990 and cybercrime risks
- Curriculum provision promotes ethical and lawful digital behaviour
- Online safety education addresses hacking, malware, phishing, denial-of-service activity and data misuse

- Learners are signposted to positive pathways for developing cyber skills
- Staff are aware of NCA Cyber Choices guidance and resources

Roles and Responsibilities

- Governors provide strategic oversight of safeguarding and cybercrime prevention.
- Senior Leaders ensure preventative education is delivered and staff are appropriately trained.
- The Designated Safeguarding Lead (DSL) assesses concerns, completes safeguarding risk assessments, maintains records and seeks external advice where appropriate.
- Technical staff monitor network use in line with the Filtering and Monitoring Policy and report concerns to the DSL.
- All staff must report suspected computer misuse immediately and reinforce legal and ethical expectations.

Identification and Reporting

Computer misuse may include:

- Unauthorised access to systems or accounts
- Attempting to bypass filtering or monitoring controls
- Use of malware or hacking tools
- Denial-of-service activity
- Password harvesting or credential sharing
- Data theft or system interference

Where concerns arise, the matter will be referred to the DSL, a safeguarding risk assessment will be completed, and parents/carers will be informed unless doing so would increase risk.

Referral to Cyber Choices

Where appropriate, the school may consult or refer to the local Cyber Choices team via the Regional Organised Crime Unit (ROCU).

Support and Risk Management

The school will ensure that:

- Risk assessments are proportionate and regularly reviewed
- Educational and behavioural support is provided
- Learners are supported to redirect technical skills positively
- Safeguarding responses are consistent with the wider safeguarding framework

Training and Awareness

The school will ensure that:

- Staff receive safeguarding updates relating to computer misuse risks
- DSLs understand referral routes and thresholds
- Governors understand oversight responsibilities
- Parents/carers are signposted to relevant guidance where appropriate

Monitoring and Review

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

Incident trends and safeguarding reviews will inform continuous improvement.

Appendix C1 – Filtering and Monitoring Policy

Purpose

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

Scope

This policy applies to:

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

Roles and Responsibilities

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

Policy Statement

The school will ensure that:

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

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

Filtering

The school will ensure that filtering systems:

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

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

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

Monitoring

The school will ensure that monitoring:

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

- Third-party monitoring software is used, that is automated and records securely kept. The software will include an access audit trail
- records will only be accessed by the OSL/DSL and retained in line with the schools data protection, retention and storage policy.

Testing, logging and review

The school will test the effectiveness of the filtering and monitoring systems, using an independent test platform, and record evidence of such tests. This will be readily available to the DSL and Chair of the governance committee. The records of the tests will include the following information:

- Date
- Reviewer
- Testing platform used
- Device tested
- networks tested (Guest, staff or student network)
- VPN/proxy testing;
- search-engine testing;
- AI services;
- identified weaknesses;
- remedial action & completion of remedial action;

Governor/SLT sign-off.

Review and Training

Filtering and monitoring provision should be reviewed at least annually and whenever risks or technologies change. Staff, governors and those with specific responsibilities will receive appropriate training.

Appendix C2 - Technical Security Policy

(including Access, Device and Incident Management)

Purpose

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

Scope

This policy applies to:

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

Policy Statement

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

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

Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights
- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect [NCSC](#) and [DfE guidance](#)
- Multi-factor authentication is used for sensitive systems where appropriate
- Administrator access is restricted and monitored

System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly

- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly, stored securely (both locally and offsite, with rotation) and regularly tested
- Physical access to infrastructure is controlled

Device Management

The school will ensure that:

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

Supplier Management

The school will ensure that:

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

Incident Management

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

Review and Training

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

Appendix C3 - Cyber Security Policy

Purpose

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

Scope

This policy applies to:

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

Policy Statement

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

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

Cyber Security Strategy

The school will maintain a cyber security strategy that:

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

Supplier Management

The school will ensure that suppliers:

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

Awareness and Education

The school will ensure that:

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

Incident Response

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

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

External Assurance

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

Review

Cyber security arrangements will be reviewed termly, or sooner if required by incidents, guidance or changes in technology. Lessons learned from managing incidents should inform improvements to the strategy. This will be discussed by the IT staff and SLT member in charge of Data protection.

Appendix C4 - Online Safety Policy | Artificial Intelligence

Introduction

The integration of Artificial Intelligence (AI) in UK schools has evolved significantly over recent years, reflecting both technological advances and the educational community's response to the opportunities and challenges it presents.

A consensus is emerging about the benefits of AI to enhance personalised learning and streamline administrative tasks, while also raising concerns around data privacy, ethical use, and the preparedness of teachers to effectively integrate AI tools into classrooms.

This ongoing dialogue reflects the recognition of AI's transformative potential in education, balanced with a need for careful implementation to protect learner welfare and promote equitable outcomes. These considerations are shaping a pathway for embedding AI in schools, focusing on teacher training, ethical guidelines, and fostering digital competency among students.

Policy on the use of Artificial Intelligence in Schools

Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

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

Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff Discipline policies and codes of conduct
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements
- Curriculum Policies

Policy Statements

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in KCSIE
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless

explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.

- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Responsibilities

Headmaster and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

The IT Manager will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may

include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be “high risk”. If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- nominated member of staff
- established school reporting mechanisms
- online/offline reporting tool
- anonymous/confidential reporting routes
- links to national or local organisations

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school’s normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing
- PHSE & Cross curricular programmes