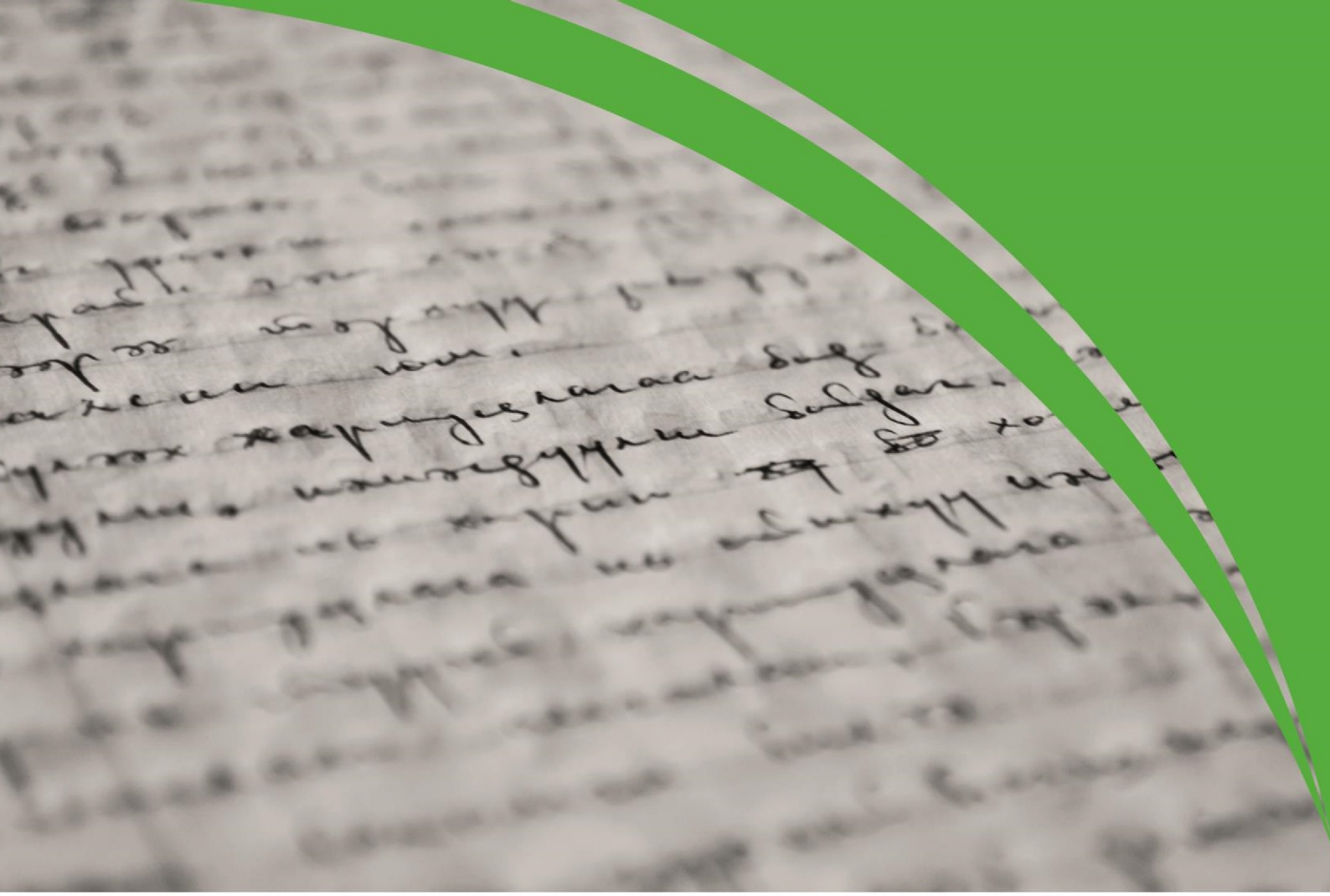


Online Safety Policy

This policy has been adopted in advance of joining the White Horse Federation on the 1st November 2026

Key Document Details

School Name:	TWHF – All Schools		
Version no:	4	Ratified date:	Sept 2026
Author:	Director of Education	Interim review date	N/A
Owner:	Director of Education	Next review date:	Sept 2027
Approved by:	CEO		

Table of Contents

Changes 3
Scope of the Online Safety Policy 4
Policy development, monitoring and review 4
Monitoring the impact of the policy 4
Policy and leadership 4
Responsibilities 5
Headteacher and senior leaders 5
Governance 5
Designated Safeguarding Lead (DSL) 5
Online Safety Lead (OSL) – this role may be a senior leader and/or the DSL 6
Curriculum Leads 6
Teaching and Support Staff 6
WHFIT / technical staff 6
Learners 7
Parents and carers 7
Community users 7
Online Safety Group 7
Membership 7
Core responsibilities 7
Policy 7
Online Safety Policy 7
What the policy does 8
Implementation, monitoring and review 8
Communication and accessibility 8
Acceptable use 8
Reinforcement 8
Acceptable/Unacceptable Actions 8
Reporting and responding 11
Introduction 11
Reporting Concerns 11
Responding to Concerns 11
Recording and Monitoring 11
External Support and Escalation 12
Use of Artificial Intelligence (AI) 12
Policy statements 12
Safe use, data protection and security 13

Quality, fairness and integrity 13
Reporting, monitoring and accountability 13
Use in assessment and feedback 13
Misuse and disciplinary action 13
Education 13
Online Safety Education Programme 13
Staff 14
Local Governors 15
External Stakeholders 15
Working with Parents and Carers 15
Wider Community and Agencies 15
Technology 16
Purpose 16
Filtering and Monitoring 16
Oversight and Review 16
Technical Security 17
Cyber Security 17
Data Protection 17
Review 18
Technology Practice 18
Purpose 18
Device Management 18
Digital Content 19
Public Online Communications 19
Review 20
Outcomes 20

Changes

Version	Date	Page document	Change	Origin of change e.g. Change in legislation, Policy review
2	September 2024	All	Improved layout to support printing and rebranded.	
3	September 2024	All	Updates in the DfE Technical Standards for Schools and Colleges, concerning filtering, monitoring and cyber-security	Change in legislation

3.1	September 2025	19	references to the use of Artificial Intelligence	Change in legislation
3.2	September 2025	33	New section on cyber-security and the use of AI in schools	Change in legislation
4	September 2026	All	Consolidated update retaining relevant Trust-specific requirements from the September 2025 policy. Strengthened governance, reporting, filtering and monitoring, AI, education, device management, cyber security, data protection, digital content and public communications.	Annual policy review; updated statutory and sector guidance; consolidation of existing Trust controls.

Scope of the Online Safety Policy

This Online Safety Policy sets out how The White Horse Federation (TWHF) 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 White Horse Federation 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 White Horse Federation (TWHF) 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.

Policy development, monitoring and review

This Online Safety Policy has be*en developed by the members of the TWHF Executive Team supported by:*
headteacher/senior leaders
Designated safeguarding leads (DSL)

Escalation following serious incidents: the school will inform the TWHF Executive Team and relevant external agencies as appropriate, including the Local Authority safeguarding lead, LADO and/or police.
Named contacts/agencies: Headteacher, DSL, Director of Education, Director of IT and Communications, Trust Data Protection Officer, Local Authority safeguarding lead, LADO and police, as appropriate.

Monitoring the impact of the policy

Each 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 each school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

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

Senior leaders will:

- Ensure each school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, WHFIT/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 WHFIT on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

Governance

Trustees and Local Governors 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 local governing committee 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 WHFIT, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the local governing committee or the relevant safeguarding committee.
- Undertake basic cyber security awareness training and support school cyber security oversight.

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 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 WHFIT and relevant external partners as required.

- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the WHFIT lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

Online Safety Lead (OSL) – this role may be a senior leader and/or the DSL

The OSL will:

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

Curriculum Leads

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

Teaching and Support Staff

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

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- 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.

WHFIT / technical staff

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

The WHFIT 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 WHFIT Service Desk at itsupport@whfit.org.uk and to the DSL where a safeguarding concern is identified.
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Learners

Learners will:

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

Parents and carers

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

Each 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.

Membership

- Director of Education
- Director of IT and Communications
- WHFIT Representative
- DSL, OSL, Senior Leader(s)

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.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Track and evidence improvement actions (e.g. 360 safe).

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 (KCSIE Para 121), 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 Acceptable Use Agreements (AUAs) AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

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

Acceptable/Unacceptable Actions

Schools should agree what is acceptable/unacceptable for their context (age, setting and systems) and record this in the tables below.

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	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
communicate material or comments that are:	• 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) *Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).*					
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 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					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	young people away from cybercrime and into positive pathways.					
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	

Reporting and responding

Introduction

Each 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.

Each 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

Each school will ensure that:

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

Responding to Concerns

Each school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

Each school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Record online safety and safeguarding incidents on CPOMS in accordance with Trust safeguarding procedures, with technical incidents also reported to WHFIT where appropriate.

- Where a device must be examined and no illegal activity is suspected, involve one or more senior staff, use a designated device, record relevant URLs and preserve evidence securely. If illegal activity is suspected, do not investigate beyond immediate safeguarding actions; preserve evidence and seek advice from police or the appropriate agency.
- Provide appropriate feedback and support to those who report or are affected by an incident, while maintaining confidentiality and safeguarding requirements.
- 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 Governors (via safeguarding reports)
    - *Staff*
    - *Learners, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners where relevant*

External Support and Escalation

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

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

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

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.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

Policy statements

Each 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

Each school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only Trust-approved or school-approved AI tools may be used for schoolwork, and staff should use Trust-provided or school-provided AI accounts where available to support oversight and reduce risk.
- Require new AI tools or services to undergo Trust approval and data protection screening before use. A Data Protection Impact Assessment will be completed where the proposed processing is likely to result in a high risk to individuals.
- 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

Each school will:

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

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the DSL, Trust Data Protection Officer and/or WHFIT as appropriate to the nature of the concern.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices in Appendix C7.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

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

Misuse and disciplinary action

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

Each 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).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

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

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff 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:
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles
- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- staff follow cyber security policy and requirements.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).

- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. ProjectEVOLVE EDU) and, where appropriate, enhanced pathways (e.g. ProjectEVOLVE SAFEGUARDING).
- 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.

Local Governors

Local Governors should take part in online safety training and awareness activity. This is particularly important for governors with responsibility for safeguarding and online safety.

Training and updates may be provided through:

- 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 so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

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

Working with Parents and Carers

Each 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/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches
- accurate, balanced and age-appropriate information about changes affecting social media and other online services
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

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

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

Technology

Purpose

Each 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 Trust 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.

Each 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 SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.

- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

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

Each 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.
- A documented access-control model is maintained and reviewed at least annually. Access is allocated on a least-privilege basis and users must protect their credentials and report suspected compromise immediately.
- Password and authentication arrangements follow current National Cyber Security Centre guidance. Multi-factor authentication is used for sensitive systems and remote access where required by Trust standards.
- Networks, servers, wireless systems, firewalls, endpoints and cloud services are securely configured, patched, protected from malware and reviewed regularly.
- Backups are maintained, tested and protected from compromise, including network-separated or otherwise appropriately isolated copies.
- School and Trust software must be appropriately licensed. Staff must not install software on school-owned devices without WHFIT approval.
- Removable media must not be used unless approved by WHFIT. Personal or sensitive data must be encrypted at rest and in transit and must not be transferred to personal devices.
- Mobile devices are managed through appropriate device-management controls, and guest access is provided according to an identified risk profile.
- Actual or suspected technical incidents and security breaches must be reported promptly to the WHFIT Service Desk.

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).

Each 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

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

The Trust ensures that:

- personal data is processed lawfully, fairly and transparently.
- a Data Protection Officer (DPO) is appointed, and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.

- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised.
- data is stored, shared and disposed of securely.
- data breaches are reported and managed in line with legal requirements.
- data protection is embedded across safeguarding, teaching, learning and administration.
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.
- The Trust maintains records of processing activities, information asset records, lawful bases, retention requirements and ownership for personal data.
- Only the minimum personal data necessary for the stated purpose is collected and retained, and personal data is kept accurate and disposed of securely in line with the retention schedule.
- Privacy notices explain how personal data is used and how individuals may exercise their rights. Procedures are maintained for Subject Access Requests and other information-rights requests.
- Appropriate due diligence and data-protection-compliant contracts are required for processors and suppliers, and data is shared only where there is a lawful basis and an appropriate secure method.
- Personal data breaches are reported internally without delay and, where legally required, to the Information Commissioner's Office within 72 hours of awareness and to affected individuals as required.
- Personal data held on authorised mobile devices or removable media must be encrypted and password protected, protected by current endpoint security, and securely deleted when no longer required.
- Staff must use secure, password-protected Trust systems, log off appropriately, use approved encrypted storage and secure transfer methods, and must not move Trust personal data to personal devices.

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

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

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

Device Management

Each 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

Each school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies

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

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

Digital Content

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

Each school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.
- Retained Trust requirements for images, video and learner work
- Images of learners must be taken using school-approved devices and systems. Personal staff devices must not be used for this purpose.
- Staff must check and respect restrictions applying to individual learners before capturing or publishing images.
- Images and recordings must be selected carefully, stored securely, retained only as required and used in accordance with the Trust retention schedule and privacy information.
- Learners must not capture, use, share or publish images or recordings of others without appropriate permission.
- Learners' full names must not be published alongside photographs or video. Learner work may be published only with the appropriate permission of the learner and parent/carer.
- Parents and carers will be informed of the purpose, storage and expected retention of images, and permissions will be obtained where required.

Public Online Communications

Each 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

Each school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.
- Retained Trust requirements for social media and online publishing
- Only authorised school accounts and approved platforms may be used for official public communication.
- Official social media accounts must have senior-leader approval, clear administration and moderation arrangements, and involvement from at least two members of staff.
- Staff must not use personal email, messaging or social-media accounts to communicate with learners or parents/carers about school business.
- Staff must not discuss personal matters relating to members of the school community on personal social media, and personal opinions must not be presented as those of the school or Trust.
- Public content must minimise personal information, protect learner identity and comply with safeguarding, copyright, data protection and image-consent requirements.
- Where concerns about the school are raised publicly, the school should encourage direct, private contact and signpost the complaints procedure where the matter cannot be resolved informally.

Review

Technology practice is reviewed regularly to reflect:

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

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes (e.g. using ProjectEVOLVE Knowledge Maps assessment and tracking). Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety.