



ICT AND INTERNET ACCEPTABLE USE POLICY

Our Mission Vision and Values

Our mission is to work with those who need us the most.

Our vision is to create a blended Trust that includes SEND schools, mainstream primary and PRUs and to create hubs that drive school improvement.

Our values are:

To be inclusive

To provide nurturing/caring environments

For children to feel safe

To work with integrity and a strong moral compass

To have the highest expectations and standards.

Approved by	Trust	
Last reviewed on	5 October 2026	
Next review due by	September 2027	Or earlier if required

The Trust digital lead coordinates digital and cyber security delivery and is the role referred to as the senior digital lead or Trust cyber security lead. Each academy must have an appointed senior leadership team digital lead.

This document is read alongside the KAT Digital Strategy 2026, KAT Cyber Strategy 2026, ICT Acceptable Use Policy 26-27, and Cyber Security Plan 26-27. The strategies set direction, the policy sets user and operational rules, and the action plan tracks implementation. Strategy or plan wording does not authorise exceptions to the approved policy. Conflicts must be escalated to the CEO for resolution and, where required, Trust Board approval.

This document must also be read alongside the KAT Use of AI Policy 2026. That policy sets the detailed rules for approved tools and uses, sensitive meetings, staff and pupil training, assessment integrity and AI-related concerns. It operates alongside the ICT Acceptable Use Policy; neither policy authorises exceptions to the other. Any proposed change to these controls requires Trust Board approval and an approved policy revision before implementation.

This policy sets the rules for safe, responsible use of digital technology across Kings Academy Trust. It protects pupils, staff and information while supporting teaching, learning, administration and communication. It applies in every Trust academy and the central team, including authorised use away from Trust premises.

Contents

- 1 Purpose scope and definitions
- 2 Legislation and guidance
- 3 Roles and responsibilities
- 4 Acceptable and unacceptable use
- 5 Staff and other adult users
- 6 Pupils parents carers and visitors
- 7 Filtering and monitoring
- 8 Data security and protection
- 9 Cyber security
- 10 Artificial intelligence
- 11 Mobile phones and personal devices
- 12 Incident reporting and response
- 13 Monitoring review and related policies

Appendix Cyber security glossary

Appendix Official sources

1 PURPOSE SCOPE AND DEFINITIONS

Kings Academy Trust provides ICT to enable education and effective Trust operations. Everyone must use it lawfully, respectfully and securely. This policy establishes common expectations, protects personal and confidential information, supports safeguarding and reduces disruption caused by misuse or cyber incidents.

It covers trustees, local governors, employees, agency and supply staff, pupils, volunteers, contractors, parents, carers, visitors and anyone given access to Trust systems or data. It applies to Trust premises, remote working, educational visits, remote education and Trust devices used at home. Use of personal devices is covered where they access Trust systems or information, or where conduct affects safeguarding, work or the school community.

ICT includes networks, internet connections, computers, tablets, phones, cloud services, email, learning platforms, websites, social media, AI tools and connected equipment. Materials include

documents, messages, images, recordings, pupil work and other digital or printed information. Personal use means activity unrelated to employment, study or the authorised purpose of access. IT support means the internal team or contracted provider authorised by the Trust.

Each academy must communicate its local arrangements, including named safeguarding contacts, IT support routes, approved platforms and mobile-phone storage arrangements. These implement this policy and must not weaken it. Accessible explanations and reasonable adjustments must enable users with additional needs to participate safely.

2 LEGISLATION AND GUIDANCE

The Trust complies with applicable law and has regard to statutory guidance. DfE digital standards describe recommended approaches; they are not all separate statutory duties. Requirements expressed as “must” in this policy are Trust rules unless expressly identified as legal duties. Official sources are linked in Appendix F.

- Safeguarding: the Education (Independent School Standards) Regulations 2014, including the welfare requirements applicable to academies; Keeping Children Safe in Education 2026 (KCSIE), in force from 1 September 2026; and the Prevent duty under the Counter-Terrorism and Security Act 2015.
- Information and privacy: UK GDPR and the Data Protection Act 2018, as amended by commenced provisions of the Data (Use and Access) Act 2025; the Human Rights Act 1998; and the Freedom of Information Act 2000. Monitoring must also satisfy applicable communications and interception law.
- Conduct and access: the Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and Equality Act 2010. Searching and confiscation must follow applicable powers under education legislation and current DfE advice; this policy creates no additional search powers.
- Operational guidance: DfE digital and technology standards, updated 16 September 2026, particularly filtering and monitoring, cyber security and digital leadership; DfE statutory mobile-phone guidance; data protection in schools; generative AI guidance and product safety standards; and relevant ICO and NCSC guidance.

3 ROLES AND RESPONSIBILITIES

Trust Board and local governance

The Trust Board approves this policy, retains overall strategic accountability and assures itself that safeguarding, information governance and cyber risks are understood and controlled. It commissions proportionate assurance, provides resources and challenges unresolved weaknesses. A designated trustee oversees assurance filtering and monitoring. Local governing bodies scrutinise implementation within the Trust’s scheme of delegation and escalate concerns; delegated scrutiny does not transfer the Board’s accountability.

Chief Executive Officer and Trust digital leadership

The Chief Executive Officer is accountable for implementation across the Trust and assigns a senior leader to coordinate digital strategy, standards and risk management. This Trust digital lead brings together educational, technical, safeguarding, finance and data-protection expertise; maintains a funded improvement programme; and reports material risks and incidents to the executive and Board.

The Trust digital lead ensures that asset, information asset and contract registers are maintained; procurement includes security and privacy checks; and digital systems are included in disaster recovery and business continuity planning. The digital strategy is reviewed annually against educational and organisational needs. Gaps against the DfE standards are recorded with owners and timescales, recognising the 2030 ambition for the six core standards without delaying existing safeguarding or security duties.

Headteachers and academy digital leads

Each headteacher is responsible for implementation in their academy, supported by an appointed senior leadership team digital lead. They provide induction and training, approve access through the agreed process, ensure supervision and publish local operating arrangements. They make sure

responsibilities, including absence cover, are assigned and that significant concerns reach Trust leaders promptly.

Designated safeguarding leads

Each designated safeguarding lead (DSL), supported by deputies, leads the safeguarding response to online concerns, understands the academy's filtering and monitoring arrangements, reviews relevant alerts and ensures appropriate action. The DSL works with IT support on risk assessment and system effectiveness, advises on curriculum access and coordinates referrals and support for children. Technical teams do not replace the DSL's safeguarding judgement.

IT support and data protection

IT support administers authorised access, secure configuration, filtering, monitoring, updates, backups and technical incident response. It maintains system documentation, records changes and reports gaps or failures to the digital lead and DSL as appropriate. Providers must have clear service expectations, escalation routes and contractual safeguards; outsourcing does not remove Trust accountability.

The Data Protection Officer (DPO) independently advises and monitors compliance, supports impact assessments and breach assessment, and is a contact for individuals and the ICO. The Trust remains accountable as controller for processing it determines. Managers and system owners implement controls and cooperate with the DPO; the DPO is not the sole owner of data security.

All users

Users must follow this policy, complete relevant training, protect access credentials, report concerns immediately and cooperate with proportionate investigations. Staff supervising pupils must teach safe practice and act on concerns. No user may assume another person has reported an incident.

4 ACCEPTABLE AND UNACCEPTABLE USE

Authorised users may use Trust ICT for teaching, learning, approved research, administration and communication appropriate to their role. They must respect others, protect information, follow licensing conditions and use only access that has been granted. Permission to use a resource does not authorise access to every file it contains.

Unacceptable activity

- Accessing, creating, storing, sending or promoting illegal or harmful material, including child sexual abuse material, terrorist content or discriminatory abuse; bullying, harassment, threats, grooming, sexual harassment or exploitation; and creating or sharing abusive impersonations or sexualised AI images.
- Making, requesting or sharing nude or semi-nude images, videos or livestreams involving children. A safeguarding disclosure or accidental receipt must be reported, not circulated. The response must prioritise the child's safety and follow section 12.
- Fraud, phishing, gambling, scams, unauthorised advertising or private commercial activity; infringement of copyright, software licences or intellectual property; plagiarism or misrepresentation of another person's or AI-generated work.
- Unauthorised disclosure of confidential information; accessing, altering, copying or deleting data without authority; sharing passwords or authentication codes; impersonating another user; or helping anyone gain unauthorised access.
- Installing software, apps, browser extensions or services without approval; connecting unapproved equipment; disabling security; using proxies, unauthorised VPNs, hotspots or other methods to bypass filtering or monitoring; or testing systems for vulnerabilities without explicit written authorisation.
- Deliberately damaging devices or systems, introducing malware, disrupting services, removing equipment or disposing of records without authority. Users must not conceal incidents or destroy potential evidence.

- Using abusive or discriminatory language, making malicious false statements, or publishing confidential Trust information through personal accounts. These rules do not prevent lawful criticism, protected disclosures, trade union activity or use of the complaints procedure.

Educational exceptions

Teaching about difficult subjects may require access to material normally restricted. Staff must request an exception in advance through the academy digital lead. The headteacher, with DSL advice and IT support, may authorise a lawful, specific, time-limited exception after considering pupils' ages, additional needs, supervision and safer alternatives. IT support records and implements the decision. No exception permits illegal material, abusive conduct or an unlawful disclosure.

Response to misuse

Access may be temporarily restricted to protect people or systems while facts are established. The headteacher or relevant Trust manager will apply the behaviour, staff conduct, disciplinary or contractual procedures fairly and proportionately. Measures may include guidance, retraining, closer supervision, restrictions or formal action; serious matters may be referred to statutory agencies. A child's vulnerability, age and additional needs must inform the response.

Restrictions must preserve necessary educational access through safe alternatives. Distinguish accidental exposure and good-faith reporting from deliberate misuse. Users may challenge decisions through the applicable behaviour, employment or complaints process. The Trust will not use a general concern about reputation to prevent legitimate reporting.

5 STAFF AND OTHER ADULT USERS

Accounts and Trust equipment

Staff, trustees, governors and other adults receive only the access needed for their responsibilities. Their manager or authorised sponsor requests access from IT support, which verifies approval and creates individual accounts. Users must report unexpected permissions and must not explore information exposed in error. Managers notify IT support promptly of role changes and leaving dates so that access can be amended or withdrawn.

Trust equipment remains Trust property. Users must keep it secure, protect it when travelling, lock screens when unattended and prevent use by family members or others. Do not leave equipment visible in vehicles or unattended in public places. Follow IT instructions for updates and shutdown, and return devices, chargers, records and access tokens when requested or when the role ends. Report loss, damage or suspected compromise immediately.

Email messages and telephone communication

Use Trust-approved accounts and channels for Trust business. Do not forward work email automatically to personal accounts or use personal email or private messaging to communicate with pupils. Do not give personal telephone numbers or email addresses to pupils or parents for work communication. Any exceptional safeguarding or emergency contact must be necessary, recorded and reported to the headteacher or DSL.

Check recipients, attachments and sharing permissions before sending. Use approved secure transfer or encryption for sensitive information and send any decryption secret through a separate channel. Use approved mailing tools or blind copying where recipients must not see each other's addresses. Independently verify unexpected requests for payments, bank changes or sensitive records through a trusted contact route.

Messages must be professional and accurate. Work records may be subject to lawful disclosure, including subject access requests and litigation; deleting an inbox message does not necessarily remove all copies. Report misdirected messages containing personal data immediately to the DPO and IT support, and follow their containment instructions. Do not use or circulate information received in error.

Call or meeting recording requires a defined purpose, an appropriate lawful basis, approval from the responsible manager with DPO advice, and advance information for participants. Recordings must

use approved systems and retention arrangements. This policy does not authorise routine call recording or covert recording.

Personal use and social media

Limited personal browsing on Trust equipment is permitted during breaks, away from pupils, where it does not affect duties, security, costs or others' access. It is subject to this policy and proportionate monitoring, and may be withdrawn. Trust email is for work. Do not use Trust storage for private collections of photographs, music or videos.

Only authorised staff may manage official social media. Protect account recovery details and apply the same approval, safeguarding and privacy checks as other publications. Personal accounts must maintain professional boundaries: do not friend, follow privately or message current pupils, discuss confidential matters or imply that personal views represent the Trust. Disclose pre-existing family or personal connections that could affect boundaries to the headteacher.

Remote working

Use only IT-approved remote access on authorised devices, with required authentication and encryption. Protect screens and conversations from being overlooked or overheard. Do not use shared public computers for Trust work, download records to personal storage or allow household members to use work sessions. Use a Trust-approved secure connection; seek IT advice before using public Wi-Fi for sensitive work.

6 PUPILS PARENTS CARERS AND VISITORS

Pupil access and online learning

Pupils use approved systems for educational purposes under arrangements appropriate to their age, maturity and needs. Teachers supervise use, explain the relevant agreement and check planned resources. Independent access, including for sixth-form pupils, must be explicitly authorised and remain subject to safeguarding controls. Specialist equipment is used only under the supervision or permission of the responsible teacher.

Accounts identify individual pupils wherever practicable. Staff may provide secure, age-appropriate sign-in support, but must not give pupils staff credentials. Pupils must not share accounts, install software or use unapproved chat, social media or AI services. They must ask for help with unexpected links, attachments, requests for money or personal details, and anything upsetting or suspicious.

Online safety teaching develops understanding of harmful content, unsafe contact, harmful conduct and commercial risks. It includes AI-generated material, misinformation, manipulation, privacy, respectful relationships, consent and routes to help. Teaching must be accessible for pupils with special educational needs and disabilities and respond to additional safeguarding vulnerabilities.

Staff explain which platforms pupils are expected to use at home, the purpose of activities and which staff or other authorised people pupils will interact with. Remote lessons use approved accounts and settings, maintain professional boundaries and follow safeguarding arrangements. Recording is permitted only where authorised and communicated. Pupils must not record or redistribute lessons without permission.

The Trust may respond to online conduct outside school where it affects pupils' safety, the school community or the orderly running of education, and where lawful powers apply. Safeguarding support and proportionate behaviour procedures apply; this is not a blanket claim to control all private online activity.

Parents and carers

Parents and carers are asked to discuss the age-appropriate agreement with their child, encourage safe use at home and report concerns to the school. Schools will offer advice and accessible alternatives where digital access is a barrier. Signing an agreement acknowledges expectations; it does not replace a lawful basis for processing personal data or constitute consent to every use of a child's information.

Use official school channels for questions, sensitive concerns and complaints. Communicate respectfully, protect other families' information and avoid naming children in discussions of incidents. Independent parent groups are not Trust channels. Parents should not publish images or recordings of other children without appropriate permission, and must observe event-specific safeguarding restrictions. Legitimate complaints and criticism remain permitted.

Visitors contractors and guest access

There is no automatic entitlement to network access. The headteacher or authorised host approves access for a defined purpose and period, and ensures the adult agreement is acknowledged. IT support provides proportionate permissions and a segregated guest service where internet-only access is sufficient. Staff must not share internal Wi-Fi credentials with unauthorised users.

Contractors require named, time-limited access appropriate to the work, with supervision or logging proportionate to risk. They must follow Trust safeguarding and information-security rules, report incidents and return or securely delete Trust data as instructed. A parent acting as a volunteer must also follow the adult agreement.

7 FILTERING AND MONITORING

The Trust uses filtering to restrict access to harmful material and monitoring to identify concerns requiring a response. These controls support supervision and education; they cannot guarantee safety or identify every incident. Mobile data, encrypted services, apps and personalised or AI-generated content can create gaps. Users must never bypass controls.

Assessment and technical controls

The DSL and IT support must assess academy needs together, including age, vulnerability, curriculum, languages, devices, home use and new services. The Trust will review provision at least once each academic year and following significant change or incident. The review must consider dynamic and AI-generated content, avoid unnecessary blocking of legitimate teaching and identify further checks. A DPIA must be completed for technical monitoring, with DPO advice and scrutiny of provider privacy information. [F2]

IT support must document the scope of protection across Trust networks, guest access and managed devices, including off-site use. Devices issued for home use must have appropriate protections or documented restrictions that prevent unsafe use. Approved search settings, browser controls and access permissions must support filtering. New services must be assessed before introduction; a block may be changed only through the authorised process in section 4.

Checks alerts and action

Each academy must maintain an operating record identifying the responsible DSL and deputy, technical provider, checking schedule, alert recipients, response cover and escalation route. IT support must check operation at the start of each term, after material changes and after reported failures, with additional checks based on risk. Record the date, tester, coverage, results and corrective action. Tests must use safe testing resources, not illegal content.

As a Trust operating requirement, the DSL or trained deputy must review safeguarding alerts on each school day and act immediately on alerts indicating urgent risk. IT support must escalate urgent findings directly, using telephone or in-person contact where an electronic message may be missed. System faults go to IT support and the digital lead; safeguarding concerns also go to the DSL. The headteacher must establish holiday and absence arrangements and clearly communicate any limits of out-of-hours coverage. Monitoring systems must also produce weekly summary reports and immediate high-risk alerts; weekly summaries do not replace daily review or urgent action.

Monitoring may include websites and searches, device and account identifiers, access logs, email or collaboration activity and content flagged by approved safeguarding or security tools. Reviewers must check context, including false positives, and record actions securely. A technical alert alone is not proof of misconduct. Access to more detailed content requires a necessary, proportionate and authorised purpose.

Privacy and transparency

Monitoring is limited to safeguarding, security, system operation, lawful investigation and legal obligations. Access is restricted to authorised personnel with a need to know and must be logged. The Trust will explain the actual systems used, information collected, who receives it, retention and off-site coverage in accessible notices. Users must receive this information before access; significant changes must be communicated.

Information must be retained only for a justified period under the Trust retention arrangements, protected against misuse and disclosed only lawfully. The DPO advises on monitoring lawfulness and privacy impact. No blanket authority to intercept communications, continuously observe private life or inspect unrelated personal content is granted. Monitoring concerns may be raised with the DPO or through complaints procedures.

8 DATA SECURITY AND PROTECTION

The Trust processes personal information under UK GDPR and the Data Protection Act 2018 as amended, including relevant commenced changes made by the Data (Use and Access) Act 2025. The 2025 Act amends the framework; it does not replace the need for lawful, fair, transparent and secure processing. Staff must follow the data protection policy, privacy notices and retention arrangements. [F6–F8]

Collect use and share information safely

- Access only the information necessary for the task. Keep records accurate, record the purpose and lawful basis through approved processes, and apply additional conditions for special-category and criminal-offence information. Ask the DPO where the basis for processing or disclosure is unclear.
- Use approved Trust storage and collaboration tools. Do not place records in personal email, private cloud accounts, consumer messaging or unapproved AI tools. Restrict shared links to identified recipients and check access before sending.
- Use secure transfer and appropriate encryption for sensitive information. Minimise attachments and copies. Collect printouts promptly, keep paper and devices secure and dispose of them through approved confidential-waste arrangements.
- Do not retain information indefinitely. Follow the retention schedule and any preservation requirement for a safeguarding matter, complaint, information request or legal proceeding. IT support must securely erase or destroy data-bearing equipment before reuse or disposal and record completion.

Access and device protection

Accounts must have the minimum permissions required. IT support reviews access at least termly and after role changes, and promptly removes access no longer needed. Administrator accounts are separate from everyday accounts. Users must lock devices when away, sign out after use and follow approved encryption and device-management requirements. Removable storage is prohibited unless IT support authorises an encrypted device and a specific business need.

Managers must ensure work records are retained appropriately when staff leave without permitting ongoing access by the departing user. Access to a former employee's mailbox or files requires authorised, proportionate arrangements with privacy safeguards. Users must not transfer a leaver's password to a replacement.

New systems suppliers and individual rights

Before procurement or significant change, the system owner must consult IT support and the DPO about security, processing contracts, hosting, international transfers, retention, access and deletion. Complete a DPIA where processing is likely to create high risk, including relevant monitoring and AI deployments. Unresolved high risks must be escalated before processing begins.

Forward information-rights requests and data-protection complaints to the DPO immediately; do not delete potentially relevant records or promise disclosure. Assess requests under the law and

applicable exemptions. Safeguarding information must be shared where necessary and lawful: data protection must not be used as a reason to withhold information needed to protect a child.

The Trust must provide an accessible route for data-protection complaints through the DPO, acknowledge complaints within 30 days, investigate appropriately and communicate the outcome without undue delay. This reflects the complaints duty in force from June 2026. Individuals may contact the ICO. A complaint acknowledgement deadline does not replace the separate deadlines for information-rights requests. [F8]

9 CYBER SECURITY

Passwords and authentication

Use strong, unique passwords or approved passkeys and keep them confidential. IT support must enforce appropriate strength and controls against repeated guessing. Staff must use the approved password manager where provided. Never disclose a password or authentication code in response to a message or approve an unexpected sign-in request. Report suspected compromise immediately and change affected credentials through the approved process.

Passwords must be changed when compromise is known or suspected, and default credentials replaced before use. Routine expiry is not required solely because time has passed. Age-appropriate and accessible sign-in methods may be approved for pupils without losing accountability. The Trust must enable multi-factor authentication for staff cloud and remote-access accounts and IT administrative accounts, with accessible alternatives where required. [F3, F12]

Defence and maintenance

IT support must maintain firewalls, supported anti-malware or endpoint protection, secure configurations and appropriate network separation. Users must not disable protections or delay instructed updates. Unlicensed or unsupported technology must be removed, replaced or isolated under an approved risk plan. The management information system and cloud services require named technical ownership and clear supplier responsibilities.

Vulnerability fixes must be applied within 14 days of release where rated critical or high, scored CVSS v3.1 7.0 or above, or unrated by the vendor. Active exploitation or other urgent threats require faster action. IT support must track and escalate exceptions, isolate exposed systems where needed and record time-limited mitigations; recording an exception does not extend the deadline. [F3]

Backups and recovery

IT support must back up critical information at least daily and maintain at least three backup copies of important data on at least two separate devices, including at least one off-site copy. Backups must be immutable and include an offline or otherwise logically isolated copy, protected so that compromised administrator credentials cannot alter every copy. Cloud storage and synchronisation alone are not a sufficient backup strategy. Recovery priorities must include safeguarding, attendance, communications, payroll and other essential services.

Test restoration at least termly and after significant system changes, recording results and remedial actions. The Trust digital lead must ensure recovery plans cover shared services and the possibility that an incident affects several academies. Keep emergency contact and recovery information accessible when normal systems are unavailable.

Awareness assurance and response planning

Staff and governors receive induction and annual cyber awareness training, with additional training for higher-risk roles. Pupils receive age-appropriate instruction. Training includes phishing, social engineering, suspicious links and attachments, payment fraud, passwords, authentication, physical security, removable media and prompt reporting. Suppliers' access and security must be assessed before appointment and through service reviews.

The Trust digital lead coordinates an annual cyber risk assessment, revisited each term and after significant change or incident. Risks have named owners and deadlines. The cyber response plan must be exercised at least annually and after a serious incident, including alternative communications

and restoration. Independent assurance of key controls is commissioned annually, proportionate to risk.

Users must report suspected attacks immediately and must not negotiate with attackers. The Trust will not pay ransom demands. The executive incident lead coordinates specialist advice, containment, evidence preservation, recovery and external notifications under section 12.

10 ARTIFICIAL INTELLIGENCE

AI tools must not be used to record, transcribe, summarise or take notes in meetings or discussions involving identifiable safeguarding or child protection information, special category personal data, or other confidential pupil or staff information. This includes uploading meeting recordings, transcripts, minutes or notes to an AI service. Use authorised non-AI arrangements for these records.

AI may support teaching, learning and administration only where it has an approved purpose and adequate safeguards. It must not replace professional accountability, safeguarding judgement or the pupil's own learning. These requirements apply to standalone tools and AI features embedded in browsers, search, office software and learning platforms.

Approval before use

The Trust AI lead coordinates approval under the Board's recorded delegation, working with the Trust digital lead with the DSL, DPO, IT support and relevant educational or service lead. Approval must identify the tool, permitted users, purpose, age limits, data permitted, supervision, retention, training use of inputs, security and safeguards. Staff must not create pupil accounts or enable new AI features without approval. Procurement must consider DfE guidance and product safety standards, including the ability to report harmful outputs. [F9–F10]

The default is to keep personal, confidential and safeguarding information out of generative AI. Any strictly necessary use of personal data requires documented Trust approval, DPO advice, an appropriate lawful basis and conditions, supplier safeguards and a DPIA where required. Pseudonymised information may still be personal data. Removing a name alone does not ensure anonymity.

Staff responsibilities

- Check outputs for accuracy, bias, appropriateness, confidentiality and copyright before use. Verify factual references against reliable sources. Do not publish or send unchecked AI output as a Trust statement or professional assessment.
- Do not upload pupils' original work for model training without the required permission or an applicable copyright exception. Review service terms; paying for a product does not automatically prevent training on inputs.
- Keep a human decision-maker accountable. The Trust does not permit solely automated significant decisions about admissions, safeguarding, behaviour, assessment or employment under this policy. Any proposed change requires separate governance and legal assessment.
- Disclose material AI assistance where needed to avoid misleading pupils, colleagues, families or assessors. Do not use AI to fabricate records, impersonate others, generate sexualised images or conceal authorship.

Pupil use and assessment

Pupils may use only approved tools, for tasks expressly authorised by their teacher, with age-appropriate supervision and safeguarding controls. They must understand that chatbots can be wrong and can simulate relationships without being a trusted adult. They must not disclose personal information about themselves or others, or rely on a chatbot for an urgent safeguarding or health concern.

Teachers must explain what assistance is permitted and how pupils should acknowledge it. Pupils must not submit AI-generated material as their own unaided work. Under the Use of AI Policy, pupils must not use AI during internal or external assessments or coursework. Staff must also follow current awarding-body rules and task instructions; teacher permission cannot override the Trust prohibition or

those rules. Suspected misuse must be assessed fairly using appropriate evidence, not an AI-detection score alone.

Unsafe outputs and review

Stop using a tool and report harmful, sexualised, discriminatory or privacy-compromising output to the teacher or DSL, and to IT support where a technical control may have failed. Preserve only safe evidence as directed; do not reproduce illegal images. Approval must be reviewed when a product's terms, capabilities or risks change. Access may be suspended while concerns are investigated.

11 MOBILE PHONES AND PERSONAL DEVICES

Each academy must maintain and communicate arrangements that prohibit pupils' use of mobile phones and other smart technology with similar functions throughout the school day, including lessons, transitions, breaks and lunchtime, subject to lawful adjustments and agreed individual exceptions. This reflects DfE statutory guidance that schools should follow from 1 September 2026. [F5]

Pupil arrangements

The academy's published mobile-phone arrangements specify whether devices may be brought in, how they are stored, collection procedures and consequences for misuse. Pupils must keep devices switched off and stored as directed. Personal hotspots and mobile data must not be used to evade controls. Wearables and smart devices capable of messaging or recording are subject to the same restrictions.

Parents needing to reach a pupil during the day should contact the school office; pupils needing to contact home should seek staff help. Schools must explain any arrangements for sixth-form pupils and ensure that they do not undermine the wider school approach. Educational visits and residential trips require clear, risk-assessed rules communicated beforehand.

Adjustments and individual needs

Headteachers must consider reasonable adjustments for disabled pupils, medical needs and exceptional individual circumstances, including caring responsibilities. A phone needed to support diabetes management, for example, must be considered within the pupil's healthcare arrangements. Agreed access must be specific about purpose, times and locations, recorded and reviewed. Staff must know the arrangement without unnecessarily disclosing the pupil's private information. [F5]

Adaptations must not be treated as misconduct. Where safe access requires an alternative device or supervised arrangement, the school will work with the family and relevant professionals. A general phone restriction must not prevent compliance with equality or medical-support duties.

Staff and visitor devices

Adults must model appropriate use. Personal phones must not distract from teaching, supervision or safeguarding. Necessary work authentication or emergency use should be brief and consistent with local arrangements. Personal devices must not be used to photograph or record pupils, or store Trust records, unless a specific arrangement has been authorised following safeguarding and data-protection assessment.

Access to Trust information from a personal device requires approval by the headteacher or relevant Trust manager and IT support, with DPO advice where needed. Approved access must use secure authentication, supported software, encryption and managed separation of work information. Trust data must not be downloaded to unmanaged personal storage. Any ability to remove work data remotely must be explained before enrolment.

Visitors must follow the host's instructions on phone use, photography and guest connectivity. Connecting to a guest network does not authorise access to internal systems or recording. Staff must use Trust-issued equipment for pupil images and work calls wherever practicable.

Searching and confiscation

Only staff with the appropriate authority may search or confiscate devices, using lawful powers and DfE guidance. Any examination of data must meet the relevant legal conditions and be necessary and

proportionate. Consult the DSL where safeguarding is involved. Do not copy, forward or delete suspected illegal images or potential criminal evidence; follow the safeguarding and police advice described in section 12. Record actions and secure confiscated property appropriately. [F11]

12 INCIDENT REPORTING AND RESPONSE

Report concerns immediately, even when the cause is uncertain or you made a mistake. Do not wait for proof or for the next working day if there is an urgent risk. A technical ticket alone is not sufficient to report an immediate safeguarding concern.

Who to contact

- Pupils: tell a teacher or another trusted adult immediately. If that adult is unavailable or the concern continues, tell another adult. Parents and visitors: contact the school office and ask for the DSL for safeguarding concerns or the relevant manager for other incidents.
- Staff: report safeguarding concerns directly to the DSL or deputy and use the school's safeguarding recording procedure. Report cyber or equipment incidents to IT support and the headteacher or Trust manager. Report any suspected personal-data breach immediately to the DPO as well as IT support; involve the DSL if children may be at risk.
- Concerns about an adult's conduct: follow the allegations and low-level concerns procedures. Report to the headteacher, or use the alternative route in the safeguarding policy if the concern involves the headteacher or a Trust leader. Do not investigate the allegation yourself.
- Immediate danger: call 999 and secure urgent help. If the DSL or deputy is unavailable, staff must follow the safeguarding policy and make a direct referral to children's social care or police where necessary. Report the action to the DSL as soon as possible.

Immediate practical action

Stop the unsafe activity. For a suspected cyber compromise, disconnect the affected device from the network if safe and within your competence, then follow IT instructions. Do not wipe, reset, run unsolicited recovery tools or power off equipment unless directed or necessary for safety. Use a known telephone number or an unaffected device if email may be compromised.

Record the time, system or device, what happened and who may be affected. Keep suspicious messages available through the approved reporting method; do not forward harmful material to colleagues. Do not investigate accounts, contact an alleged offender, negotiate with an attacker or make public statements.

If a child discloses harmful content or imagery, listen, reassure and report without blame. Do not promise secrecy. Staff must not ask a child to send or show nude or semi-nude images, or copy or forward them. Leave decisions about any exceptional viewing to the DSL under safeguarding guidance. Preserve devices and other safe evidence without spreading the material.

Coordinated response and external reporting

The executive incident lead coordinates major incidents across affected academies. The DSL leads child-protection action; IT support leads technical containment and recovery; the DPO advises on personal-data risk and notifications. The Trust records decisions, maintains essential services and communicates through authorised channels without exposing confidential information.

The Trust must notify the ICO of a personal-data breach without undue delay and, where feasible, within 72 hours of awareness unless it is unlikely to result in a risk to individuals' rights and freedoms. High-risk breaches also require notification to affected individuals without undue delay, subject to legal exceptions. Incomplete information must not delay an initial required report; reasons for delay and decisions not to notify must be recorded. [F13]

The incident lead arranges any required reports to police, Report Fraud, the DfE sector cyber team and the NCSC as applicable and insurers or the risk protection arrangement, and considers contractual notification duties. Every serious incident must have a lessons-learned review with tracked corrective actions and Board oversight.

13 MONITORING REVIEW AND RELATED POLICIES

Putting the policy into practice

Headteachers and Trust managers must make this policy available to all users and explain it during induction. All staff must read KCSIE 2026 Part One in full and receive safeguarding training, including online safety. The relevant agreement is completed before access, with an age-appropriate explanation and support where needed. Schools must keep acknowledgement records securely and refresh them following material changes. Visitors may acknowledge the adult agreement electronically as part of access arrangements.

Each academy must keep its operational information current and accessible: safeguarding contacts and deputies, the IT support route, DPO contact route, approved learning services, monitoring notices and device arrangements. The school office must be able to direct any user to the relevant contact. Contact details and technical products are maintained operationally so that changes do not leave this policy with outdated information.

Assurance and review

The Trust digital lead coordinates monitoring with headteachers, DSLs, IT support and the DPO. At least termly, leaders consider incidents and near misses, access reviews, training completion, filtering checks, alert handling, cyber risks, outstanding fixes and feedback from users. Reports to governors and trustees should protect individuals' identities unless their details are necessary for the governance purpose.

At least annually, the Trust Board reviews this policy and receives assurance on implementation, including filtering and monitoring effectiveness, cyber preparedness and significant data-protection issues. The CEO must ensure that gaps have an owner, resources and a completion date. The DPO retains independence when reporting compliance concerns.

An earlier review is required following a serious incident, a material change to technology or monitoring, significant legislative or guidance changes, or evidence that the policy is not working. The next scheduled review is September 2027. Substantive changes require Trust Board approval and must be communicated to affected users.

Related policies and procedures

This policy must be read alongside the current Trust and academy arrangements covering:

- Safeguarding and child protection, online safety, Prevent and allegations or low-level concerns about adults.
- Behaviour, anti-bullying, mobile phones, special educational needs and disabilities, equality and support for medical conditions.
- Staff code of conduct, social media and communications, disciplinary procedures and whistleblowing.
- Data protection, privacy notices, information-rights requests, data breaches, records retention, photography and recording.
- Remote education, assessment and examinations, AI use where separately documented, procurement, business continuity and cyber incident response.
- Complaints and visitor or contractor arrangements.

Current documents are available through the Trust or academy's published policy channels or from the school office; staff-only procedures are provided through internal channels. A separate local procedure may add detail but must not reduce the protections in this policy. Where there is uncertainty, users must seek advice from the responsible leader before proceeding, except where immediate safeguarding action is needed.

APPENDIX CYBER SECURITY GLOSSARY

These terms explain common risks and safeguards used in this policy.

AI and generative AI Artificial intelligence refers to systems performing tasks such as prediction or content generation. Generative AI creates material such as text, images, audio or video.

Anti-malware and antivirus Software that detects, blocks or removes malicious software. Endpoint protection adds controls on individual devices.

Cloud service A service or storage system accessed over a network and operated on remote infrastructure. The Trust must still manage access, contracts and data protection.

Cyber attack and cyber incident An attack is a deliberate attempt to compromise technology or information. An incident is an event affecting or threatening its confidentiality, integrity or availability.

Data breach A security failure leading to accidental or unlawful loss, destruction, alteration, disclosure of or access to personal data. It is not limited to hacking.

DPIA A data protection impact assessment identifies and reduces privacy risks before and during relevant processing.

Encryption Protection that makes information unreadable without the necessary key or authorised access.

Firewall A control that permits or blocks network traffic according to security rules.

Malware virus and Trojan Malware is harmful software. A virus can replicate itself; a Trojan disguises harmful functions as legitimate software. Untrusted downloads may install malware.

MFA and passkeys Multi-factor authentication checks identity using different types of evidence. A passkey is a cryptographic sign-in method that can reduce phishing risks.

Patching and penetration testing Patching fixes or updates software. A penetration test is a specifically authorised assessment of security weaknesses; users must not test Trust systems independently.

Phishing spear phishing and whaling Deceptive messages try to obtain information or trigger unsafe action. Spear phishing targets particular people; whaling targets senior decision-makers.

Pharming and social engineering Pharming redirects a user to a fraudulent website. Social engineering manipulates people into revealing information or taking unsafe action.

Ransomware Malware that blocks access to systems or information, often through encryption, and may threaten disclosure to demand payment.

VPN A virtual private network provides an encrypted connection. Only approved VPNs may be used for Trust access; unauthorised VPNs must not bypass controls.

APPENDIX OFFICIAL SOURCES

Official sources checked on 24 September 2026. Links below support the policy's legal and guidance basis. Operational frequencies and approval rules adopted by KAT are Trust controls and do not imply that every detail is prescribed by legislation.

F1 Keeping Children Safe in Education 2026

DfE statutory guidance in force from 1 September 2026. All staff must read Part One in full. Online safety, including AI-related risks, is addressed within the whole-school safeguarding approach.

F2 Filtering and monitoring core standard

DfE recommended approach to safeguarding expectations. Updated 16 September 2026; includes annual review, emerging content risks and DPIAs for technical monitoring.

F3 Cyber security core standard

DfE recommended approach to cyber resilience, including acceptable use, risk assessment, authentication and timely vulnerability fixes.

F4 Digital leadership and governance core standard

DfE guidance on leadership, registers, continuity planning and digital strategy. This is one of the six core standards towards which schools should work by 2030.

F5 Mobile phones in schools

Guidance became statutory on 29 June 2026; schools should follow it from 1 September 2026. The detailed guidance addresses restrictions, reasonable adjustments and exceptional circumstances.

F6 Data protection in schools

DfE practical guidance supporting the application of data-protection law in schools, including AI and information management.

F7 Data Use and Access Act commencement

Government commencement information. Apply provisions in force; the Act does not abolish UK GDPR or the Data Protection Act 2018.

F8 Data protection complaints duty

ICO confirmation of the complaints duty, including a clear reporting route, acknowledgement within 30 days, appropriate investigation and communication of the outcome.

APPENDIX OFFICIAL SOURCES CONTINUED

F9 Generative AI in education

F10 Generative AI product safety standards

F11 Searching screening and confiscation in schools

F12 NCSC password administration for system owners

F13 ICO personal data breaches guide

Legislation

Read legislation as amended and in force. The sources below provide the principal statutory framework referred to in section 2; they do not create a general authority to inspect personal devices or intercept private communications.

UK General Data Protection Regulation

Data Protection Act 2018

Data Use and Access Act 2025

Education Independent School Standards Regulations 2014

Counter Terrorism and Security Act 2015

Computer Misuse Act 1990

Copyright Designs and Patents Act 1988

Equality Act 2010

Children and Families Act 2014 section 100

Human Rights Act 1998

Freedom of Information Act 2000

Education Act 1996 searching powers

Education and Inspections Act 2006 discipline powers

Telecommunications Lawful Business Practice Interception of Communications Regulations 2000