The Willows School Academy Trust



ICT and Acceptable Use Policy

Reviewed: September 2026

Next Review: September 2027

Introduction & Aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can compromise the safe and effective running of the school. Breaches of this policy may be dealt with under our staff code of conduct and behaviour policy.

Relevant Legislation & Guidance

This policy refers to, complies with, or otherwise has regard to, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2026
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges
- The Crime and Policing Act 2026

Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, Chromebooks, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **Making or sharing of nudes or semi-nudes:** creating, possessing, or distributing images or videos (including those digitally altered or wholly generated by artificial intelligence) depicting nudity or semi-nudity of any person under 18 years of age
- **Biological sex:** a person's sex as recorded at birth (male or female)

See appendix 4 for a glossary of cyber security terminology.

Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination (including misogyny or misandry)
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Making or sharing of nudes or semi-nudes (including images digitally altered or wholly generated by artificial intelligence such as deepfakes). All incidents involving making or sharing of nudes or semi-nudes will be treated as safeguarding matters requiring an immediate response, regardless of whether the images are real, altered, or AI-generated.
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Use of AI not in line with our E-Safety policy and safe use of AI guidance
- Inputting sensitive information, personal data, or confidential school information into third-party AI systems without authorisation
- Using mobile phones in contravention of the school's mobile phone-free environment policy

- Using digital systems to facilitate access to facilities designated for the opposite biological sex
- Using digital systems to record or change a pupil's biological sex without proper authorisation
- Attempting to authorise, process, or approve financial transactions without proper authorisation or in breach of the trust's scheme of delegation

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from Unacceptable Use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on staff code of conduct and behaviour policy.

Specific sanctions may include:

For pupils:

- Verbal warning
- Loss of ICT privileges for a specified period
- Confiscation of personal devices
- Parents/carers contacted
- Behaviour sanctions in line with school behaviour policy
- In serious cases, fixed-term or permanent exclusion

For staff:

- Verbal or written warning
- Suspension of ICT access
- Disciplinary action up to and including dismissal
- Referral to external agencies (police, Teaching Regulation Agency) where appropriate

All incidents involving making or sharing of nudes or semi-nudes will be treated as safeguarding matters and referred immediately to the Designated Safeguarding Lead (DSL).

Staff (including governors, volunteers, and contractors)

5.1 Access to School ICT Facilities and Materials

The school's leadership and ICT team manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, Chromebooks, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Co-ordinator or member of SLT immediately.

All staff access is subject to monitoring in accordance with section 5.5 of this policy.

5.1.1 Use of School-Supplied Equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required.

Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that the screen and documents are not visible to others
- Lock devices with a password when unattended. Passwords must:
    - Not be shared with others and must be changed regularly (at least twice per year)
    - Be suitably strong, in accordance with the school's password policy (see section 8.1)

    - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the ICT coordinator
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a school device promptly to the ICT co-ordinator, a designated safeguarding lead and data protection officer
- Not use school devices to access facilities designated for the opposite biological sex
- Ensure any use of AI tools complies with the school's E-Safety policy and AI guidance

5.1.2 Use of Phones and Email

The school provides each member of staff with an email address.
This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.
Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.
Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
Email messages are required to be disclosed in legal proceedings or in response to subject access requests from individuals under the UK GDPR and the Data Protection Act 2018 in the same way as paper documents.
Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted using a strong, state-of-the-art encryption standard so that the information is only accessible by the intended recipient.
If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
If staff send an email in error that contains the personal information of another person, they must inform a member of SLT and ICT Co-ordinator immediately and follow our data breach procedure.
Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the school to conduct all work-related business.
School phones must not be used for personal matters.
Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.
The school can record incoming and outgoing phone conversations.
Callers must be made aware that conversations are being recorded. The school's phone system has an automated message informing callers that calls may be recorded for training and quality purposes.
Staff who would like to record a phone conversation should speak to a member of SLT.
All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.
Requests to record conversations may include when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

Staff must not use personal mobile phones during the school day except during designated break times and in designated areas (staff room, offices). Staff must not use personal mobile phones in areas where pupils are present.

5.1.3 Trustee and Governor Access

Trustees and governors will be provided with appropriate access to school ICT systems to fulfil their governance responsibilities, including:

- Access to governance documents and papers
- Access to monitoring and reporting systems as required for their role
- Secure email accounts for trust/school business

Trustees and governors must:

- Complete cyber security awareness training annually
- Use MFA for all access to school systems
- Only access systems and data relevant to their governance role
- Not share login credentials
- Report any security concerns immediately to the headteacher and trust leadership

The trust's scheme of delegation defines which systems and data trustees and governors may access.

5.2 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff use their personal devices (such as mobile phones or tablets) in line with the school's code of conduct and E-Safety policy.

Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of email (see section 5.1.2) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Social Media Accounts

Members of staff should make sure their personal use of social media – whether for professional or private purposes – is appropriate at all times and complies with school guidance.

The school has guidelines for staff on appropriate security settings for social media accounts.

Staff must ensure that:

- Privacy settings are set to maximum
- They do not accept friend/connection requests from current pupils or parents/carers
- They do not make reference to the school, pupils, parents/carers or colleagues on personal social media
- They do not post anything that could bring the school into disrepute
- They are aware that even with privacy settings, content can be shared and become public
- They do not engage in online discussions about school matters on personal accounts

5.3 Remote Access

We allow staff to access the school's ICT facilities and materials remotely through freedom2roam, which is monitored by the London Grid for Learning (LGFL).

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions to avoid compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

When accessing school systems remotely, staff must:

- Use the approved VPN (Virtual Private Network) connection
- Ensure they are working in a private space where screens cannot be overlooked

- Lock devices when stepping away
- Log out completely when finished
- Not allow family members or others to use school devices or access school systems
- Report any technical issues or security concerns immediately

5.4 Use of Artificial Intelligence (AI) Tools
Staff may only use AI tools that have been approved by the school.
When using approved AI tools, staff must:
- Only use school-provided AI accounts configured for educational use
- Never input sensitive information, personal data, or confidential school information into AI systems
- Always fact-check and critically evaluate AI-generated content before use
- Clearly label any content that has been created or influenced by AI
- Ensure human oversight and final decision-making, particularly for matters affecting pupils
- Be transparent about AI use with colleagues, pupils and parents where appropriate
- Understand that AI should assist, not replace, professional judgement
- Report any concerns about AI outputs (including bias, inaccuracy, or inappropriate content) immediately
- Never use AI to generate or manipulate images of pupils, staff or any identifiable individuals
- Follow the school's E-Safety policy regarding AI use

Unauthorised use of AI tools, or misuse of approved AI tools, will be treated as a breach of this acceptable use policy and may result in disciplinary action.

5.5 Monitoring and Filtering of the School Network and Use of ICT Facilities
To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network.
This includes, but is not limited to, the filtering and monitoring of:
- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
Pupils are monitored internally through the use of Google for Education Admin console, and websites are monitored and filtered at the request of staff and parents.
The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:
- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.
The school monitors ICT use in order to:
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- Identify and respond to safeguarding concerns, including the making or sharing of nudes or semi-nudes

Filtering and Monitoring Review:
In accordance with KCSIE 2026, the school conducts a mandatory review of filtering and monitoring systems at least once every academic year.

This review is conducted by the Senior Leadership Team (SLT) member responsible for filtering and monitoring, supported by the Designated Safeguarding Lead (DSL) and IT support. This review assesses the effectiveness of filtering and monitoring in identifying risks, evaluates whether systems are appropriately configured for different user groups, and ensures that safeguarding concerns (including attempts to access, create, or share inappropriate content) are being identified and escalated appropriately."
Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this includes how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) and ICT co-ordinator take lead responsibility for understanding the filtering and monitoring systems and processes in place.
Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.
Where Generative AI is used to support monitoring, human oversight is maintained to interpret nuances and context that AI might miss.

Pupils

6.1 Access to ICT Facilities

- ICT equipment is available to pupils only under the supervision of staff
- Email addresses and passwords are provided to pupils, for educational purposes only. Pupils must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content, without the permission of the ICT co-ordinator
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using their school Google login
- Pupils must adhere to the school's mobile phone-free environment policy at all times

6.2 Pupil Responsibilities
Pupils are responsible for:

- Using school ICT facilities in accordance with the pupil acceptable use agreement
- Keeping passwords secure and not sharing them with others
- Reporting any concerns, inappropriate content, or bullying to a trusted adult immediately
- Treating equipment with care and respect
- Not attempting to bypass filtering or security measures
- Following instructions from staff regarding ICT use
- Not bringing mobile phones into school (or if permission has been granted for travel safety, handing phones to the office upon arrival)
- Not creating, possessing, or sharing nudes or semi-nudes (including AI-generated images)
- Understanding that all online activity is monitored for their safety

6.3 Unacceptable Use of ICT and the Internet Outside of School
The school will sanction pupils, in line with our behaviour policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Making or sharing of nudes or semi-nudes (including images digitally altered or wholly generated by artificial intelligence such as deepfakes). The school will respond to all incidents of making or sharing nudes or semi-nudes with a safeguarding response, working with parents/carers, and where appropriate, external agencies including police and children's social care.
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Using AI in ways not permitted by the school's policies

All incidents involving making or sharing of nudes or semi-nudes will be treated as safeguarding matters and handled in accordance with KCSIE 2026 guidance.

6.4 Education and Support

The school will:

- Provide age-appropriate education on online safety through the curriculum
- Teach pupils about the risks and consequences of unacceptable use
- Provide support to pupils who experience online bullying or other online safety issues
- Work with parents/carers to promote consistent messages about online safety
- Educate pupils about the serious nature of making or sharing nudes or semi-nudes, including AI-generated images
- Teach pupils about the school's mobile phone-free environment and the reasons for it

6.5 Recording of Biological Sex and Social Transition

The school is legally required to record a pupil's biological sex accurately in all systems and records.

Staff must:

- Record biological sex (male or female) as registered at birth in the school's management information system (MIS) and all official records
- Not make any changes to how a pupil's sex is recorded without explicit authorisation from the headteacher and involvement of parents/carers
- Not initiate any action regarding a pupil's social transition
- Only respond to requests for social transition support if specifically requested by the child or their parents/carers
- Involve parents/carers in any decisions relating to social transition, except in exceptionally rare cases where doing so would pose a greater risk to the child
- Exercise particular caution regarding requests for social transition in primary schools, where full social transition should be agreed very rarely
- Report any requests or concerns regarding social transition to the Designated Safeguarding Lead (DSL) immediately

Pupils must not:

- Access digital facilities, records, or systems designated for the opposite biological sex
- Attempt to change or request changes to their recorded biological sex in school systems without parental involvement

Parents/ Carers

7.1 Access to ICT Facilities and Materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy and sign the appropriate acceptable use agreement.
Parents/carers acting as volunteers must comply with the school's volunteer policy and safeguarding procedures. In accordance with The Crime and Policing Act 2026 and KCSIE 2026, any volunteer who frequently teaches, trains, instructs, or supervises children is in regulated activity and requires an enhanced DBS check with children's barred list information.

7.2 Communicating with or About the School Online
We believe it is important to model for pupils, and help them learn and promote, how to communicate respectfully with, and about, others online.
Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.
We ask parents/carers to:

- Be respectful in all communications with the school, staff, and other parents/carers
- Not use social media to complain about or criticise the school, staff, or other parents/carers
- Follow the school's complaints procedure if they have concerns
- Not share photos or videos of other children without permission from their parents/carers
- Support the school's online safety education
- Support the school's mobile phone-free environment policy
- Understand that the school will inform them immediately if their child is involved in any incident involving making or sharing of nudes or semi-nudes, or if there are serious online safety concerns
- Model appropriate online behaviour for their children

7.3 Communicating with Parents/Carers About Pupil Activity
The school will ensure that parents and carers are kept informed of any online activity that their children are being asked to carry out.
This information will be shared through the usual homework reporting system so parents or carers are well informed. In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.
Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.
The school will inform parents/carers immediately if:

- Their child is involved in an incident involving making or sharing of nudes or semi-nudes
- Their child has been the victim of online bullying
- There are serious concerns about their child's online safety
- Their child has breached the acceptable use policy in a serious way

---

Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.
Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software
- Regular security updates and patches
- Encrypted data transmission and storage
- Secure backup systems

8.1 Passwords
All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.
Strong passwords must:

- Be at least 8 characters long (12+ characters recommended)
- Include a mix of uppercase and lowercase letters, numbers, and symbols
- Not be based on easily guessed information (names, birthdays, common words)
- Not be reused across different accounts
- Be changed regularly (at least twice per year for staff)

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.
Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.
Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.
Multi-factor authentication (MFA) is required for:

- All staff accounts accessing sensitive data
- Remote access to school systems
- Access to financial systems
- Access to the school's management information system (MIS)

Multi-factor authentication (MFA) is mandatory for:

- All staff accounts accessing sensitive data
- Remote access to school systems
- All access to financial systems, including:
    - Banking systems and payment platforms
    - Purchase ordering systems
    - Payroll systems
    - Budget management systems
- Access to the school's management information system (MIS)

No exceptions to MFA for financial systems will be permitted, in accordance with the Academy Trust Handbook requirements for financial controls and fraud prevention.

8.2 Software Updates, Firewalls and Anti-Virus Software
All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.
Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from ICT co-ordinator.
Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
Any incoming files should always be virus-checked by the ICT co-ordinator before they are downloaded.
Any personal devices using the school's network must all be configured in this way.
The school will:

- Maintain up-to-date anti-virus software on all devices
- Apply security patches and updates promptly
- Conduct regular vulnerability assessments
- Monitor for suspicious activity
- Maintain firewall protection on all network entry points

8.3 Data Protection
All personal data must be processed and stored in line with data protection regulations and the school's data protection policy, which can be found on the school website.
The school complies with:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Data (Use and Access) Act 2025

Key principles:

- Personal data will only be collected, used, and stored for legitimate educational purposes
- Data will be kept secure and confidential
- Data will only be shared with those who have a legitimate need to access it
- Data will be kept accurate and up to date

- Data will not be kept longer than necessary
- Individuals have rights regarding their personal data

Staff must:

- Only access personal data they are authorised to access
- Not share personal data inappropriately
- Report any data breaches immediately
- Follow the school's data protection policy
- Complete data protection training
- Be particularly careful when using AI tools not to input personal or sensitive data

8.4 Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT co-ordinator.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT co-ordinator immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

The school operates a principle of least privilege:

- Users are only given access to the systems and data they need for their role
- Access rights are reviewed regularly (at least annually)
- Access is removed promptly when no longer required (e.g., when staff leave)
- Temporary access for visitors or contractors is time-limited

Staff must not:

- Share login credentials with others
- Access systems or data they are not authorised to use
- Attempt to gain elevated privileges without authorisation
- Leave systems logged in and unattended

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT co-ordinator.

Encryption requirements:

- All portable devices containing school data must be encrypted
- All emails containing sensitive or personal data must be sent via secure, encrypted systems
- USB drives used for school purposes must be encrypted
- Data transmitted over the internet must use secure, encrypted connections (HTTPS, VPN)
- Backup data must be encrypted

Staff must not:

- Store school data on unencrypted personal devices
- Send sensitive data via unencrypted email
- Use unencrypted cloud storage for school data
- Remove data from school premises without authorisation and appropriate encryption

8.6 Removable Media

The use of removable media (USB drives, external hard drives, CDs/DVDs) poses security risks.

The school's policy on removable media:

- Use of personal USB drives on school systems is prohibited unless specifically authorised
- School-provided USB drives must be encrypted
- All removable media must be scanned for viruses before use
- Removable media should not be used to store personal or sensitive data unless encrypted
- Lost or stolen removable media must be reported immediately
- Removable media from unknown sources must never be connected to school systems

Protection for Cyber Attacks

The school will:

- Work with governors, the IT department and external agencies such as Trailblaze to make sure cyber security is given the time and resources it needs to make the school secure

- Provide annual training for all users, including staff, pupils and governors (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including:
    - The methods hackers use for tricking people into disclosing personal information, including phishing
    - Online safety and password security
    - Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
    - The physical security of devices, for example not leaving a laptop unlocked and unattended
    - The risks of using removable storage media, such as USBs
    - Multi-factor authentication
    - How and when to report a cyber incident or attack
    - How and when to report a data breach
    - Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
    - How to check the sender address in an email
    - How to respond to a request for bank details, personal information or login details
    - How to verify requests for payments or changes to information
    - Recognising AI-generated phishing attempts and deepfakes
    - The risks of inputting sensitive data into AI systems
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate:** the school will verify this using a third-party agency such as Trailblaze to objectively test that what it has in place is effective
    - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data and store these backups on cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
    - Report suspicious emails immediately without clicking links or downloading attachments
    - Verify unusual requests (especially for payments or data) through a separate communication channel
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems

- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials (or a similarly effective and recognised) certification
- Ensure all ICT procurement follows the trust's procurement policy and scheme of delegation
- Conduct due diligence on all ICT suppliers, including:
    - Financial stability checks
    - Data protection compliance verification
    - Cyber security certification (Cyber Essentials or equivalent)
    - References from other educational institutions
- Ensure all contracts with ICT suppliers include appropriate data protection, security, and liability clauses
- Maintain a register of all third-party suppliers with access to school systems or data
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred
- The school will report a personal data breach via the ICO website. The school will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step
- Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment

9.1 Recognising and Responding to Cyber Threats

All staff should be vigilant for signs of cyber-attacks, including:

Phishing emails:

- Unexpected emails asking for personal information, passwords, or payment details
- Emails with urgent or threatening language
- Emails from unfamiliar senders or with suspicious sender addresses
- Poor spelling and grammar
- Suspicious links or attachments
- Requests to verify account details
- **AI-generated emails that may appear more sophisticated and personalised**

Malware indicators:

- Unexpected pop-ups or error messages
- Slow computer performance
- Programs opening or closing automatically
- Files appearing, disappearing, or being encrypted
- Unusual network activity

Social engineering attempts:

- Unexpected phone calls requesting information or access
- People claiming to be from IT support asking for passwords
- Requests to install software or grant remote access
- Pressure to act quickly without verification

If you suspect a cyber-attack:

1. Do not click on links or open attachments
2. Do not provide any information
3. Do not delete the suspicious email (it may be needed as evidence)
4. Report it immediately to the ICT Co-ordinator and Headteacher
5. If you've clicked a link or provided information**,** report it immediately and change your passwords
6. Disconnect from the network if you suspect your device is infected
7. Follow the school's incident response plan

9.2 Cyber Incident Response

In the event of a cyber incident, the school will:

1. **Contain the incident:**
    - Isolate affected systems
    - Prevent further spread

    - Preserve evidence
2. **Assess the impact:**
    - Determine what data or systems are affected
    - Identify who needs to be informed
    - Assess whether it's a data breach requiring ICO notification
3. **Notify relevant parties:**
    - ICO (within 72 hours if personal data breach)
    - Police (if criminal activity suspected)
    - Parents/carers (if pupil data affected)
    - Staff (if staff data affected)
    - LA and DfE (as appropriate)
    - Insurance provider
4. **Recover and restore:**
    - Remove malware
    - Restore from backups
    - Verify system integrity
    - Reset passwords
5. **Review and learn:**
    - Investigate how the incident occurred
    - Update policies and procedures
    - Provide additional training if needed
    - Implement additional security measures

9.3 Business Continuity and Disaster Recovery
The school maintains a business continuity plan that includes ICT disaster recovery procedures to ensure:

- Critical systems can be restored within defined timeframes
- Teaching and learning can continue during ICT outages
- Communication channels remain available during incidents
- Financial systems remain secure and operational

The business continuity plan:

- Is reviewed annually by the headteacher and trust leadership
- Is tested at least annually using scenario-based exercises
- Identifies critical systems and their recovery priorities
- Defines roles and responsibilities during incidents
- Includes contact details for key personnel and suppliers

Critical systems include:

- Management Information System (MIS)
- Financial systems
- Email and communication systems
- Safeguarding and child protection records
- Filtering and monitoring systems

Internet Access

The school's wireless internet connection is secure and protected by industry-standard encryption.
10.1 Pupils

- Pupils are permitted to access the school's Wi-Fi for their Chromebook for educational purposes only
- All pupil internet access is filtered and monitored
- Pupils must only access the internet under staff supervision
- Pupils must follow the acceptable use agreement at all times
- Pupils must not use mobile phones to access the internet during the school day, in line with the school's mobile phone-free environment policy

10.2 Staff

- Staff have access to the school's Wi-Fi for professional purposes
- Staff must ensure they are using secure connections when accessing sensitive data
- Staff must not share Wi-Fi passwords with unauthorised individuals

- Staff accessing the internet remotely must use the approved VPN

10.3 Parents/Carers and Visitors

Parents/carers and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Where access is granted:

- Visitors must sign the acceptable use agreement
- Access will be time-limited
- Access will be to a separate guest network with restricted access
- All activity will be logged and monitored

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10.4 Filtering and Monitoring

The school uses robust filtering and monitoring systems to:

- Block access to inappropriate content
- Prevent access to illegal content
- Protect pupils from harmful material
- Monitor for safeguarding concerns
- Detect potential security threats

Filtering categories include:

- Pornography and sexually explicit content
- Violence and hate speech
- Extremist content
- Illegal content (drugs, weapons, etc.)
- Gambling sites
- Social media (except for approved educational use)
- Malware and phishing sites
- AI tools not approved by the school
- Sites or tools that could be used to create, alter, or generate images of individuals (deepfake tools, image manipulation sites) unless specifically approved for educational purposes

The filtering system:

- Is regularly reviewed and updated
- Can be adjusted for different user groups (staff, pupils, age groups)
- Logs all filtering decisions
- Allows for appropriate educational overrides with authorisation

Monitoring systems:

- Track internet usage in real-time
- Flag concerning searches or access attempts
- Alert designated staff to potential safeguarding issues
- Maintain logs for investigation purposes
- Monitor for attempts to create, access, or share nudes or semi-nudes

Review process:

In accordance with KCSIE 2026, the school conducts **a** mandatory review of filtering and monitoring systems at least once every academic year, led by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support.

Monitoring & Review

The headteacher and ICT co-ordinator monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year, or sooner if:

- There are changes to relevant legislation or statutory guidance

- There is a significant cyber security incident
- New technologies are introduced that require policy updates
- Following a review of filtering and monitoring systems
- At the request of the governing board

The governing board is responsible for approving this policy.

Monitoring of policy implementation includes:

- Regular review of incident logs
- Analysis of filtering and monitoring reports
- Staff and pupil feedback
- Audit of access controls and permissions
- Review of training effectiveness
- Assessment of cyber security measures

The governing board will:

- Receive an annual report on ICT acceptable use and online safety
- Review the effectiveness of filtering and monitoring systems
- Ensure adequate resources are allocated to cyber security
- Ensure staff receive appropriate training
- Monitor compliance with this policy

Related Policies

This policy should be read alongside the school's policies on:

- E-Safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Data protection
- Artificial Intelligence (AI)
- Cyber security
- Mobile phone policy
- Social media policy
- Complaints policy
- Volunteer policy
- Acceptable use agreements (staff, pupils, parents/carers)
- Scheme of Delegation
- Financial Regulations/Financial Procedures Manual
- Procurement Policy
- Business Continuity Plan

Policy Approved By:
Signed: Malcolm Shaw (Headteacher)

Date: September 2026
Next Review Date: September 2027