ACE Derbyshire Trust

Acceptable Use Policy

Approved by:	Executive Team	**Date:** November 2026
Last reviewed on:	November 2026	
Next review due by:	November 2027	

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 4
5. Staff (including governors, volunteers, and contractors) 5
6. Pupils 9
7. Parents/carers 10
8. Data security 10
9. Protection from cyber attacks 11
10. Internet access 12
11. Monitoring and review 13
12. Related policies 13
Appendix 1: Acceptable use of the internet: agreement for parents and carers 14
Appendix 2: Acceptable use agreement for older pupils 15
Appendix 3: Acceptable use agreement for younger pupils 16
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors 17
Appendix 5: Glossary of cyber security terminology 18
Appendix 6: Acceptable Use poster for schools 18

1. Introduction and 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 communication systems may have a detrimental impact on the Trust, its schools, employees, pupils, and reputation. Any breach of this policy may be treated as a disciplinary matter and will be dealt with in accordance with the Trust's Disciplinary Policy, Code of Conduct, AI Policy, and any other relevant policies or procedures.

2. Relevant legislation and 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 2025
- 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

3. Definitions

- **ICT facilities**: all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, mobile phones, radios, walkie-talkies, wearable technology, software, websites, web applications, cloud services and any device, system or service that may become available in the future which is provided as part of the Trust's ICT and communications 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

See appendix 5 for a glossary of cyber security terminology.

4. 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
- 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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
- Using unauthorised artificial intelligence (AI) tools or services, or using authorised AI tools in a manner that breaches the Trust's AI Policy, Data Protection Policy, confidentiality requirements or professional standards.

The use of Artificial Intelligence (AI) is governed by the Trust's AI Policy. Users must only use AI tools that have been authorised by the Trust and must comply with all requirements set out in the AI Policy.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The CEO 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 there is a legitimate educational, operational or business need, exceptions to this policy may be authorised by the Headteacher, CEO or another appropriately authorised senior leader. Any such exceptions will be subject to appropriate safeguarding, cybersecurity, data protection and operational controls.

The use of Artificial Intelligence (AI) tools is governed by the Trust's AI Policy. Any exception relating to the use of AI tools must be considered in accordance with that policy and any associated approval processes.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust Disciplinary Policy, Code of Conduct, AI Policy, and any other relevant policies or procedures.

Copies of these policies are available from the school office.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The Trusts IT provider, ATOM IT manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, 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 ATOM IT as soon as possible by contacting support@atomit.co.uk or by calling 0115 6950000.

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 other passengers may be able to read any documents displayed on the screen of your device

Lock devices with a password when unattended. Passwords must:

- Not be shared with others and must be changed immediately if there is reason to believe they have been compromised.
- 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 our IT provider.

- 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 IT provider, designated safeguarding lead and data protection officer as a matter of urgency.

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. Staff must make sure multi-factor authentication is enabled on their email account(s).

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 the Headteacher immediately and follow our data breach procedure. To reduce this risk, staff are encouraged to make use of available email safety features, such as delayed sending, recall functions and recipient verification tools, where these are available. These features can help reduce the risk of emails being sent in error and provide an opportunity to identify and correct mistakes before information is disclosed.

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.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Radios and walkie-talkies may be used for operational, educational, safeguarding and health and safety purposes. Users must ensure communications remain professional, appropriate and limited to information necessary for the safe operation of the school or activity. Personal information about pupils, staff or families should not be transmitted unless it is necessary to safeguard a child or manage an immediate health and safety issue. Users should assume that transmissions may be overheard by others and should exercise appropriate discretion at all times.

5.1.3 Use of Personal Devices for Photography, Video and Audio Recording

Staff should ordinarily use Trust- or school-issued devices when taking photographs, videos or audio recordings of pupils.

The use of personal devices for photography, video or audio recording is only permitted where:

- there is a legitimate educational, safeguarding or operational need;
- a school-issued device is not reasonably available;
- permission has been granted by the Headteacher or a delegated senior leader;
- appropriate parental permissions are in place.

Examples may include educational visits, residential visits, forest school activities, emergency situations, or other activities where a school device is unavailable or impractical to use.

Where personal devices are used:

- only the minimum images, recordings or information necessary should be captured;
- images, videos and recordings must not be shared through personal messaging apps, personal cloud storage or personal social media accounts;
- content must be transferred to an approved Trust system as soon as practicable and no later than the end of the next working day;
- content must then be permanently deleted from the personal device, including any recycle bin, deleted items folder or cloud-synchronised storage;
- any loss, theft or compromise of a device containing Trust information must be reported immediately in accordance with the Trust's data breach procedures.

School communication devices, including walkie-talkies and radios used on educational visits, remain subject to the requirements of this policy regarding professionalism, safeguarding and confidentiality

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 CEO 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 contact time
- 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 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 use of social media, either for work or personal purposes, is appropriate at all times.

The Trust's Social Media Policy and associated guidance are available from the school office. Staff should ensure they are familiar with the requirements set out within these documents.

5.3 Remote access

The Trust permits staff to access approved Trust systems, applications and information remotely where this is necessary for their role. Remote access must only be undertaken using Trust-approved systems and accounts. Staff must comply with all applicable security requirements, including the use of strong passwords, multi-factor authentication and appropriate safeguards to protect confidential and personal information.

Staff accessing Trust systems remotely must take reasonable steps to ensure that information cannot be viewed by unauthorised individuals and that devices used to access Trust systems are secure.

Staff accessing Trust systems remotely are subject to the same expectations and requirements contained within this policy as those accessing systems on Trust premises. Staff must be particularly vigilant when accessing Trust systems

outside the school environment and must take reasonable precautions to protect information and maintain system security. This includes ensuring devices are password protected, keeping software updated, securing devices when not in use, and taking care that confidential information cannot be viewed by unauthorised individuals.

Staff must immediately report any loss, theft or suspected compromise of devices or accounts used to access Trust systems. Information held within Trust systems may be confidential and/or subject to data protection legislation. Such information must be treated with extreme care and handled in accordance with the Trust's Data Protection Policy.

Further information on the handling and protection of personal data can be found within the Trust's Data Protection Policy, which is available through the school's approved document management systems or from the school office on request.

5.4 School social media accounts

Each school and the Trust may operate official social media accounts. Responsibility for managing these accounts rests with designated and authorised members of staff. Staff who have not been authorised to manage or post content on official social media accounts must not access, or attempt to access, those accounts.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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. The Trust and its schools use a range of filtering and monitoring solutions, including systems provided by approved third-party suppliers. These arrangements are reviewed regularly to ensure compliance with safeguarding, data protection and cybersecurity requirements.

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

Our trust 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 will include 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) will 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 IT provider, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are 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 Headteacher
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

6.2 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
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 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

Breaches of this section will be considered in line with the school's Behaviour Policy and may result in appropriate sanctions being applied.

7. 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.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, 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 sign the agreement in appendix 1.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

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.

8. 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 cyber crime 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

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.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Users must keep passwords confidential and change them immediately if they believe a password may have been compromised.

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.

Staff should use the Trust-approved password manager to generate and securely store passwords where this is available. Where pupil accounts require passwords to be created by staff, these should be generated using secure methods and

stored securely until they are issued to pupils or their parents/carers. Password records must be protected from unauthorised access.

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 ATOM IT.

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.

Users should exercise caution when opening files received from external sources. Any suspicious files, links or attachments should not be opened and should be reported to the Trust's IT support provider or Data Protection Officer in accordance with local procedures.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's Data Protection Policy. A copy of the Trust's Data Protection Policy is available from the school office on request.

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 ATOM IT.

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 our IT provider 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.

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 our IT provider.

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The trust will:

- Work with directors, governors and the IT department 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, directors 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:

i. The methods hackers use for tricking people into disclosing personal information, including phishing
ii. Online safety and password security
iii. Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
iv. The physical security of devices, for example not leaving a laptop unlocked and unattended

v. The risks of using removable storage media, such as USBs
vi. Multi-factor authentication
vii. How and when to report a cyber incident or attack
viii. How and when to report a data breach
ix. Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
x. How to check the sender address in an email
xi. How to respond to a request for bank details, personal information or login details
xii. How to verify requests for payments or changes to information

- 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:

i. **Proportionate**: Filtering and monitoring arrangements will be reviewed regularly by the Trust and individual schools to ensure they remain effective, appropriate and compliant with statutory safeguarding requirements.
ii. **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
iii. **Up to date:** with a system in place to monitor when the school needs to update its software
iv. **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be

- Back up critical data - The Trust adopts a 3-2-1 backup strategy, maintaining at least three copies of critical data, stored on two different types of media, with at least one copy held separately from the live environment. Backup arrangements are designed to support business continuity, disaster recovery and protection against data loss, corruption and cyber security incidents.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ATOM IT.

Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- 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
- 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.
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred
- Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment

10. Internet access

10.1 Pupils

The school's wireless internet connection is secured through appropriate technical and organisational controls.

Separate network access arrangements are maintained for staff, pupils and visitors. Access to visitor wireless networks is restricted and protected by password controls. Visitor access credentials may be obtained from the school office or other authorised member of staff.

The Trust and its schools use filtering and monitoring systems to support safeguarding, online safety and cyber security requirements. The specific systems used may vary between schools. Users should be aware that filtering systems are not infallible and must immediately report any inappropriate content, security concern, or legitimate website that has been incorrectly blocked to a member of staff or the school's ICT support provider.

All users must comply with the school's acceptable use requirements when accessing the internet through school-provided networks.

10.2 Parents/carers and visitors

Parents/carers and visitors may be provided with access to the school's visitor wireless network where there is a legitimate educational, operational or business reason connected with their visit. Access credentials will be issued by an authorised member of staff and may be time-limited or subject to appropriate restrictions.

11. Monitoring and review

The headteacher and IT provider 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.

12. Related policies

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

- Online Safety Policy
- Social Media Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Disciplinary Policy
- Data Protection Policy
- Remote Education Policy
- Artificial Intelligence (AI) Policy
- Visits Policy
- Bring Your Own Device Policy

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page • Email/text groups for parents (for school announcements and information) • Class Dojo Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a school-related behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people • Use artificial intelligence (AI) chatbots, such as ChatGPT, Google Gemini, or CoPilot to create images or write for me, and then submit it as my own work I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access any illegal or inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the Headteacher, and ATOM IT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. Many of these terms are from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses with the end aim of fixing them.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails or text messages sent to many people asking for sensitive information (such

TERM	DEFINITION
	as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly-targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

DIGITAL SAFETY

Staff quick guide • Acceptable Use Policy

Protect pupils. Protect information. Stay professional.

✓ DO

- Use Trust email and approved systems for work.
- Keep pupil, staff and Trust information confidential.
- Use strong passwords and multi-factor authentication.
- Lock your screen when you step away.
- Check email recipients, links and attachments.

✗ DON'T

- Share passwords or use someone else's account.
- Use personal email or personal cloud storage for school business.
- Access information you are not authorised to view.
- Install unapproved software or bypass security controls.
- Share pupil images through personal social media accounts.

AI: TWO TOOLS ONLY

Microsoft Copilot • Google Gemini

Only these AI tools may be used for Trust business. Follow the Trust AI Policy.

- Check outputs for accuracy, bias and suitability. Apply professional judgement.
- Do not put confidential or personal information into unauthorised AI tools. Follow Trust data-handling rules.

PHOTOS & PERSONAL DEVICES

Use Trust devices wherever possible. Personal devices should only be used in exceptional circumstances when authorised or where necessary, such as an emergency.

Transfer school-related information, photographs and videos to Trust systems and delete them from personal devices in line with the policy's requirements.

SEE IT? REPORT IT IMMEDIATELY

Phishing • Data breaches • Lost or stolen devices • Suspected unauthorised access

Follow school reporting procedures. Report safeguarding concerns to the designated safeguarding lead (DSL).

Trust systems may be monitored. This quick guide does not replace the full Acceptable Use Policy or related policies.

Staff reference • November 2026