Bradford Diocesan Academies Trust

ICT ACCEPTABLE USE POLICY

Issued: May 2016
Reviewed: September 2026
Next Review Due: September 2027

Bradford Diocesan Academies Trust

Table of Contents

1. Trust Policy Statement

Bradford Diocesan Academies Trust (BDAT) recognises the vital role that Information and Communication Technology (ICT) plays in enriching teaching, learning and the wider educational experience. BDAT are committed to fostering a safe, respectful and effective digital environment. This policy outlines the expectations for acceptable use of ICT systems, networks, devices and digital resources across the Trust, ensuring that all users engage with technology in ways that protect individuals, data and infrastructure, whilst supporting educational excellence and operational efficiency.

As part of our focus on diversity and inclusion, BDAT pledges that our policies will seek to promote equality, fairness, and respect for all staff and pupils. Our policies reflect the BDAT values of inclusion, compassion, aspiration, resilience and excellence. By working closely with a range of key stakeholders, including our schools, unions and HR colleagues, we have ensured that the Trust's policies do not unlawfully discriminate against anybody.

For the purpose of this policy, the term 'Trust' refers to BDAT. The term school and the term academy are interchangeable. The term pupil and the term student are interchangeable.

2. Introduction and Aims of the Policy

Information and Communications Technology (ICT) is a fundamental part of how BDAT and our schools operate. It underpins teaching, learning, safeguarding, pastoral care and administrative functions, serving as a vital resource for pupils, staff, governors, trustees and visitors.

When used effectively, ICT has the power to transform education, enabling more engaging, inclusive and personalised learning experiences. From interactive platforms and digital collaboration tools to secure data systems and online resources, technology empowers our school communities to work more creatively, efficiently and collaboratively.

Based on BDAT's *Digital Vision for Excellence*, the Trust believes that digital technology, when used responsibly, can remove barriers and open doors for every child. At BDAT we want every child, regardless of background, personal characteristics, academic ability or additional need to have the chance to succeed and excel.

However, with these opportunities come responsibilities. The use of ICT must reflect the Trust's ethos and values, promoting respect for others and safeguarding the integrity of our systems. Users must avoid any actions that could disrupt services, compromise data protection, safeguarding, or impact online safety.

This Acceptable Use Policy outlines the principles and expectations for using ICT across the Trust. Aligned to the DfE's Digital and Technology standards, it aims to ensure that all users engage with technology in a safe, respectful and purposeful manner, protecting individuals, data and infrastructure from misuse and harm.

This policy covers users of Trust ICT facilities and applies to all staff, including the Board of Trustees, Governors and Central Staff, paid staff, volunteers and sessional workers, agency staff, students or anyone working for and on behalf of BDAT.

This Acceptable Use policy aims to:

- **Safeguard children and young people** by ensuring that all ICT use within BDAT schools supports a safe, secure and age-appropriate digital environment.
- **Protect the integrity, security and reliability** of the Trust's ICT systems, ensuring compliance with legal, regulatory and data protection requirements.
- **Support compliance with the DfE's Digital and Technology standards** and other recognised good practice frameworks for educational technology and information security.
- **Provide clear guidance** on the acceptable use of ICT resources and online services across all BDAT schools.
- **Establish expectations for online conduct**, helping to prevent cyberbullying, misuse and disruption.
- **Support and reinforce the Trust's safeguarding, online safety and data protection policies**, ensuring that digital practices contribute positively to pupil wellbeing and protection.
- **Prevent disruption, misuse or unauthorised access** of Trust ICT systems that could negatively impact teaching, learning, administration, safeguarding or business continuity.
- **Equip pupils and staff with the skills, knowledge and understanding** to use technology safely, ethically and effectively.

Breaches of this policy may be dealt with under the BDAT Disciplinary Policy and Procedure and/or relevant school Behaviour Policy.

3. Relevant Legislation and Guidance

This policy adheres to relevant legislation and national guidance, including, but not limited to:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Keeping Children Safe in Education 2026
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- DfE Meeting digital and technology standards in schools and colleges

This policy should also be read in conjunction with our school specific Online Safety Policy, Behaviour Policy, Safeguarding and Child Protection Policy, Anti-Bullying Policy, Mobile phone usage, Artificial Intelligence (AI) Policy, Social Media Policy, Disciplinary Policy, along with other relevant Trust level policies held on the BDAT website.

4. Policy Scope

This ICT Acceptable Use Policy applies to all individuals who access, use, manage, or support BDAT ICT systems, services, devices, networks, applications and data. This includes employees, agency and temporary staff, contractors, consultants, volunteers, governors, trustees, trainees, visitors and any other authorised users.

The policy applies to the use of all BDAT-owned, leased, or managed ICT equipment and services, as well as personal devices used to access BDAT systems, networks, email, cloud services, or data. It applies whenever ICT resources are used for BDAT-related purposes, whether on academy premises, at home, whilst travelling, or at any other location.

All users are responsible for understanding and complying with the requirements set out in this policy and any related BDAT policies, procedures, and statutory obligations.

5. General Code of Practice

BDAT provides a range of ICT systems, devices and services to support teaching, learning and business operations. All users are expected to use these resources responsibly, securely and in accordance with this Acceptable Use Policy. The requirements below are designed to maintain the security, availability and effective operation of ICT services for all users.

Topic	Requirement
Availability of Services	ICT services are generally available throughout the academic year. Planned maintenance may occasionally require systems to be unavailable outside normal working hours or during school holidays.
Backup and Data Protection	Users are responsible for ensuring that important work is stored in approved Trust locations that are subject to backup arrangements where provided. Personal data, particularly special category data, must not be stored on unencrypted media. Any physical copies containing confidential or personal information must be stored securely and disposed of in accordance with Trust retention and disposal procedures.
Connecting Devices and Equipment	Only authorised devices and peripherals may be connected to Trust equipment or networks. Users must not connect personal hardware, USBs or alter device configurations without prior approval from AIT. Approved removable storage devices may only be used in accordance with Trust procedures and security requirements.
Copyright, Intellectual Property and Plagiarism	Users must respect copyright, intellectual property rights and software licensing requirements. Material belonging to others must

	not be copied, reproduced, distributed or presented as their own work without appropriate permission or attribution.
File Transfers and Data Handling	Files may only be transferred to external devices, cloud services or third parties where there is a legitimate business need and appropriate authorisation. Users must ensure that copyright, licensing, confidentiality, data protection and information security requirements are always observed.
Food and drink	Food and drink should be kept away from ICT equipment wherever possible to prevent damage. Users must take reasonable care of all ICT equipment and maintain a safe and tidy working environment.
Logging Off and Device Security	When leaving a workstation unattended, you must lock your screen. At the end of each session, you must sign out or log off fully and ensure the device returns to the login screen before leaving it unattended.
Mobile Phones, personal devices and wearable tech	Staff use of mobile phones and personal devices must be professional, responsible and compliant with safeguarding, data protection and confidentiality requirements. Staff must not give their personal number to parents/carers or pupils. Staff must use phones provided by the Trust to conduct all work-related business. Trust phones must not be used for personal matters. Mobile phones should not disrupt teaching, learning, meetings, or other professional duties, and staff must ensure that any work-related communication is always secure and appropriate.
Passwords, User Accounts and Authentication	You will be provided with individual account credentials which must remain confidential and must not be shared with anyone else. Passwords must comply with the Trust's password requirements set out at Section 8 of this Policy. Any suspected compromise, disclosure or misuse of an account must be reported immediately to the AIT Helpdesk. You must not use another person's account, permit another person to use your account, or attempt to bypass authentication controls. All activity undertaken using your credentials will be considered your responsibility.
Personal Use	Limited personal use of ICT resources may be permitted provided it does not interfere with work duties, incur significant cost, reduce system performance, compromise security, or breach any Trust policy.
Physical Security of Equipment	Users are responsible for taking reasonable care of ICT equipment and must not leave devices unattended in unsecured locations.
Printing	Printing facilities should be used responsibly and only for legitimate school or Trust purposes. The Trust reserves the right to monitor printing activity to ensure the efficient and cost-effective use of resources.
Professional Conduct	When using ICT systems, you must act in accordance with BDAT values, policies and professional standards. ICT facilities must not be used in any way that could disrupt services, compromise security, cause offence, or adversely affect other users.
Remote Working	When working remotely, users must take reasonable steps to protect Trust information from unauthorised access, including securing devices, using approved systems, and preventing others from viewing confidential information.

Reporting Faults and Incidents	Technical faults, service disruptions, security concerns or suspected breaches must be reported to the AIT Helpdesk as soon as possible, providing sufficient detail to support investigation and resolution.
Software Installation and System Changes	Users must not install, download, uninstall or modify software, applications or system settings unless authorised by AIT. Unlicensed, unauthorised or unsupported software must not be used on Trust devices or networks.
Storage and File Management	Users are responsible for managing their allocated storage responsibly by removing redundant files and emails when no longer required. Requests for additional storage must be supported by a legitimate business need and approved by AIT.
Unauthorised Access and Security Testing	You must not attempt to access systems, data, files, applications or network areas for which you do not have permission. Any attempt to identify, exploit or circumvent security controls is strictly prohibited. The use, possession or distribution of hacking tools, password crackers, network scanners, keyloggers, packet sniffers or similar software is forbidden unless explicitly authorised by AIT for legitimate business purposes.
Use of Personal Devices (BYOD)	Personal devices may only be used to access Trust systems where explicitly authorised and configured in accordance with Trust security requirements.
Viruses, malware and security threats	Any suspected malware infection, phishing attempt, security incident or unusual system behaviour must be reported immediately to the AIT Helpdesk. Users must not attempt to investigate, remove or remediate security threats without authorisation.

6. Internet Code of Practice

BDAT provides internet access through Trust-managed devices, authorised personal devices connected to the Trust network and wireless services. Internet access is an important tool that supports teaching, learning, communication and the day-to-day work of the Trust.

When using the internet on Trust systems, networks or devices, all users are expected to do so responsibly, professionally and in a way that reflects BDAT values. This Internet Code of Practice is designed to help protect users, ensure the security of Trust systems and information, and comply with legal and safeguarding requirements.

Users should take reasonable care when accessing websites, downloading files, sharing information online and communicating electronically. Activities that could compromise the security of Trust systems, expose users to inappropriate content, breach data protection requirements, infringe copyright, or damage the reputation of the Trust must be avoided.

The Trust monitors and filters internet access in line with its safeguarding, security and legal obligations. Users should have no expectation of privacy when using Trust systems and networks.

Failure to comply with this Code of Practice may result in the restriction or removal of internet and ICT access and may lead to disciplinary action in accordance with Trust policies. Serious breaches may also be referred to external agencies or law enforcement where appropriate. The Trust reserves the right to recover any costs or losses resulting from deliberate or negligent misuse of its systems.

Topic	Requirement
Artificial Intelligence (AI) Tools	Users must only use AI tools approved by the Trust and in line with the Trust's Artificial Intelligence Policy. Users must not enter personal, confidential, safeguarding-sensitive or commercially sensitive information into public AI systems without explicit authorisation. All AI-generated content remains the responsibility of the user and should be reviewed for accuracy and appropriateness.
Cloud Services	Only Trust-approved cloud services may be used to store, process or share Trust information. Users must not upload Trust data to personal cloud storage platforms or unauthorised online services.
Copyright and Intellectual Property	Users must respect copyright, licensing and intellectual property rights. Material obtained from the internet may only be copied, downloaded, stored, adapted or shared where permitted by law, licence terms or the copyright owner. Appropriate attribution should be provided where required.
Hardware, Software and Browser Settings	Users must not modify device settings, security controls, browser configurations or installed software without authorisation from AIT. These controls are in place to protect users, devices and Trust systems from cyber security threats.
Inappropriate material	Users must not intentionally access, store, transmit or share material that is illegal, offensive, discriminatory, extremist, sexually explicit, violent, abusive, or otherwise inappropriate, including online betting and gambling. This includes content that would be unsuitable for pupils or could bring the Trust into disrepute. If inappropriate content is accessed accidentally, close it immediately and report the incident to the AIT Helpdesk or a member of the safeguarding team as appropriate.
Misuse of Online Services and Security Controls	Users must not misuse online services, attempt to bypass security controls, filtering or monitoring systems, access restricted content, or engage in activities that may compromise the security, integrity or availability of Trust systems or data.
Monitoring and Filtering	To meet its safeguarding, legal and security obligations, the Trust uses Smoothwall Monitor and Smoothwall Filter to monitor and filter internet usage on its networks and devices. Internet activity may be logged and reviewed where necessary for operational, safeguarding, security, disciplinary or legal purposes, in accordance with Trust policies and applicable legislation.
Personal Safety and Online Communication	Users should exercise caution when communicating online and only engage with individuals and organisations for legitimate educational or business purposes. Personal details, locations and other sensitive information should not be shared unnecessarily. Staff must always maintain appropriate professional boundaries.
Sharing Information Online	Users must take care when sharing information online and must not disclose confidential, personal or sensitive information relating to the Trust, its pupils, parents, staff, governors or trustees unless authorised and there is a legitimate business reason for doing so.
Social Media use	Please refer to BDAT's Social Media Policy
Use of the internet	Internet access is provided primarily to support teaching, learning and Trust business activities. Limited personal use is permitted provided it is reasonable, lawful, does not interfere with your duties, consume excessive resources, or conflict with Trust policies.

7. Email Code of Practice

The email system provided by BDAT enables staff, pupils, governors, trustees, volunteers, contractors and other authorised users to communicate efficiently with individuals and organisations both within and outside the organisation.

As email is an official Trust communication tool, all users are required to use it responsibly, securely, and in accordance with this Policy and Code of Practice. This document sets out the standards, expectations and rules governing the use of the email system.

Any breach of this Policy may be treated as a serious matter and could result in disciplinary action, withdrawal of access privileges, legal proceedings, or, in the case of pupils, sanctions up to and including exclusion. Where a breach results in financial loss, reputational damage, liability, or other costs being incurred, the Trust reserves the right to seek recovery of such costs from the individual responsible, where appropriate and permitted by law.

Topic	Requirement
Attachments and Downloads	Users must only open attachments and download files from trusted sources. Software, executable files or other unapproved content should not be introduced to the network without prior authorisation. Any suspected malware, phishing attempt or security concern should be reported immediately to the AIT Helpdesk.
Auto-Forwarding	Automatic forwarding of Trust emails to personal or external email accounts is not permitted unless approved by AIT and senior leadership.
Confidential Information	Confidential or sensitive information must be always handled appropriately. Users should verify recipients before sending messages, use approved security measures where required, and take particular care when accessing email remotely or in public locations. Confidential emails and attachments should be retained only for as long as necessary.
Email use	The email system is provided primarily to support the educational, administrative and operational activities of the Trust. Users should ensure that email is used professionally, responsibly and in accordance with all relevant policies and procedures. Staff should be mindful that emails may be disclosed under data protection legislation, or used as evidence in investigations or legal proceedings.
External Communications	Staff should take care when communicating with parents, carers, suppliers, partners and external agencies. Emails should be accurate, professional and consistent with Trust policies and values.
Inappropriate Use	Email must not be used to access, create, store or distribute offensive, inappropriate or unlawful material. Users must not engage in bullying, harassment, plagiarism, or the sharing of unnecessary personal information relating to themselves or others. Any inappropriate email or attachment received should be reported to the AIT Helpdesk.

Message size	Attachments are subject to system size limits. Where larger files need to be shared, approved cloud storage or file-sharing solutions should be used – advice can be provided by AIT.
Monitoring	To maintain security, safeguard users and ensure compliance with organisational policies, email records, including sender, recipient, date and time information, may be retained and monitored where appropriate. Access to email content will be restricted to authorised personnel and undertaken in accordance with applicable legislation and organisational procedures.
Out-of-Office Messages	Staff should use out-of-office notifications when absent for an extended period and provide an alternative contact where appropriate. Automatic responses should not contain excessive personal information.
Personal Email Accounts	Trust business should be conducted through authorised email accounts only. Personal email accounts must not be used for official communications unless specifically authorised.
Phishing and Fraud Prevention	Users should remain vigilant for phishing, suspicious links, unexpected attachments and requests for financial or personal information. Any suspected phishing attempt should be reported immediately to the AIT Helpdesk.
Professional Standards	Emails are official records of the Trust and should be written with the same care, accuracy and professionalism as any other formal correspondence. Users should consider confidentiality, data protection requirements, retention obligations and the potential disclosure of messages under legal or regulatory processes. Copyright must be respected. Emails or attachments that are offensive, discriminatory, harassing, defamatory, threatening or otherwise inappropriate are not acceptable and may result in action being taken under relevant policies and procedures.
Security	Email should not be considered a fully secure method of communication. Messages may be delayed, intercepted, misdirected or affected by technical issues. Users must take appropriate care when sending sensitive information and should never send passwords via email.
Spam, bulk-emails and distribution lists	Users should avoid sending unnecessary mass emails. Messages sent to large distribution groups should have a legitimate business purpose and, where required, be approved by an appropriate manager or senior leader. Care should be taken when using distribution lists. Staff should ensure recipients have a legitimate need to receive the information and consider the use of BCC where appropriate to protect privacy.
Storage and Retention	Users are responsible for managing their mailbox appropriately. Emails that are no longer required should be deleted in accordance with the Trust's Data Retention Schedule, while important records should be retained or archived as necessary. The organisation may apply retention periods and automated deletion processes in line with its records management arrangements.
Trust Disclaimer	The standard email disclaimer applied automatically to outgoing messages must not be removed, amended or disabled without authorisation.

Viruses and Malware	Users should remain vigilant for suspicious messages, links and attachments. Any suspected virus, malware infection or phishing email should be reported to the AIT Helpdesk immediately.

8. Passwords and Data Security

The Trust is committed to maintaining a robust and secure digital environment to safeguard its systems, staff and students. The Trust will ensure that appropriate security measures and procedures are in place to protect our computing resources, data and user accounts. These measures are regularly reviewed and updated to respond to the evolving nature of cyber threats.

All users must maintain strong, secure passwords and keep them confidential. Each user will be provided with a unique username and password, which must not be shared, disclosed or used by anyone else.

In line with National Cyber Security Centre (NCSC) guidance, BDAT does not routinely require users to change their passwords unless there is reason to believe that an account or password has been compromised. Some third-party systems used by the Trust may have their own password expiry requirements, which users must follow. Users should create strong, unique and memorable passwords, for example by using three random words, and should avoid predictable information such as names, dates of birth, keyboard patterns or common phrases. Passwords must not be shared with others and should not be reused across multiple accounts.

Password Requirements

- Minimum of 8 characters.
- Unique to each account.
- Avoid predictable information

Users must immediately report any suspected password compromise, disclosure or loss through the AIT Helpdesk.

To help maintain the security of Trust systems and information, users are expected to keep their login details and passwords confidential and secure. Where account credentials are not adequately protected or are shared with others, the Trust may take appropriate steps to mitigate any risks, including restricting access to systems, providing further guidance or training, or applying disciplinary measures in line with relevant Trust policies.

9. Monitoring and Privacy

BDAT is committed to promoting the safe, secure and effective use of ICT systems across the Trust. To protect pupils, staff, data, technology resources, and to meet its safeguarding, legal and regulatory obligations, the Trust operates appropriate monitoring and security measures across its networks, devices and online services. The Trust reserves the right to monitor, record and review the use of its ICT systems, networks, devices, internet access, email services, cloud platforms and other digital resources. This includes the use of web filtering and monitoring technologies, including Smoothwall Filter and Smoothwall Monitor, which support the Trust in safeguarding pupils and staff, identifying potential online safety concerns, investigating breaches of policy, and maintaining the security and

integrity of Trust systems. Users should be aware that activity conducted using Trust ICT systems may be monitored and recorded.

Whilst the Trust will try to respect user privacy, where there is a legitimate business, safeguarding, disciplinary, legal, regulatory, or security reason to do so, the Trust may access, review and disclose information held on or transmitted through its ICT systems. This may include emails, files, internet usage records, system logs, and other electronic communications. Information may be shared with appropriate senior staff, auditors, regulatory bodies, law enforcement agencies, or other authorised organisations where required by law, to protect the safety of individuals, to investigate suspected misconduct or criminal activity, or to support legal proceedings. Any monitoring and processing of personal data will be undertaken in accordance with applicable data protection legislation and the Trust's GDPR and Data Protection Policy.

10. Cyber Security

BDAT is committed to maintaining a secure and resilient digital environment that prioritises cyber security at every level. This includes using secure, cloud-based systems for data storage and communication, enforcing strong password policies and multi-factor authentication, with regular software updates to patch vulnerabilities. AIT continuously monitor systems for suspicious activity and respond swiftly to threats.

All users have a shared responsibility to protect BDAT systems, data and information from cyber threats. All users are required to complete the Trust's approved National Cyber Security Centre (NCSC) cyber security awareness training on an annual basis and must follow established security procedures, including the use of strong passwords, multi-factor authentication where provided, prompt reporting of suspected security incidents and vigilance against phishing, malware and other cyber-attacks. By working together and adhering to good cyber security practices, we help safeguard the confidentiality, integrity and availability of BDAT's ICT resources.

11. Policy Review

BDAT's Head of Corporate Projects is responsible for the management and oversight of the Trust-wide ICT Managed Service. This includes monitoring the implementation of this policy and ensuring it remains aligned with the evolving needs of the Trust. This policy will be reviewed annually in conjunction with the Digital Link Trustee to reflect the rapid and ongoing developments in ICT.

Appendix 1 – ICT Acceptable Use Agreement

Please sign the below to confirm you have read and understood the Trust's ICT Acceptable Use Policy:

BDAT - ICT Acceptable Use Agreement	
Employee (print name):	
Employee Agreement: I confirm that: • I have read, understood and agree to comply with the Trust's ICT Acceptable Use Policy. • I will use the Trust's ICT systems, computer network, internet access, e-mail, and other technologies responsibly, professionally and in accordance with the requirements set out in this Policy. • I understand that my use of the Trust's ICT systems, including network activity, email communications, internet access and stored data, may be monitored, logged and reviewed in accordance with the Trust's policies and applicable legislation.	
Signed:	**Date:**