Policy and Procedure

Acceptable Use Policy
(Staff, Governors, Contractors)

Reviewed and approved by:

Trust Board

Approval Date:

15 May 2025

Review Date:

15 May 2027

Version:

1

Contents

1. Policy Overview and Scope 3
1.A Policy purpose 3
1.B Intended Audience 3
1.C Policy Ownership and Review Cycle 3
2. Legal and Regulatory Framework 4
3. Roles and Responsibilities 5
3.A The Trust Board 5
3.B IT Director and IT Service Delivery Manager 5
3.C Designated Safeguarding Lead (DSL) 5
3.D Staff, Governors, Supply Staff, and Volunteers 5
3.E Third-Party Contractors and Service Providers (where applicable) 5
3.F Data Protection Officer (DPO) 5
References 6
4. Acceptable Use Expectations 7
4.A General Expectations 7
4.B Use of Accounts and Passwords 7
4.C Use of Personal Email Accounts 7
4.D Email and Communication 7
4.E Internet and System Access 8
4.F Social Media and Public Communications 8
4.G Device Use and Security 9
4.H Compliance 9
5. Use of Personal Devices (BYOD) 10
5.A General Expectations 10
5.B Security and Compliance 10
5.C Acceptable Use 10
6. Monitoring and Filtering 11
6.A Purpose of Monitoring 11
6.B Methods of Monitoring 11
6.C User Awareness and Consent 11
6.D Personal Devices 11
References 12

Appendix 1 – BCWCAT Staff Acceptable Use Agreement (AUA) 13
BCWCAT Trust Staff Acceptable Use Agreement 2025 13
Appendix 2 – Key Definitions 15
Version Control 16

1. Policy Overview and Scope

1.A Policy purpose

The purpose of this policy is to establish clear expectations and responsibilities for the appropriate, safe, and lawful use of technologies, information, and other resources. It is designed to protect users, data, and infrastructure while ensuring compliance with legal, regulatory, and safeguarding obligations. It also underpins the Trust's commitment to promoting responsible digital conduct, safeguarding users and data, ensuring legal compliance, supporting effective teaching and operations through secure technologies, and clearly defining acceptable and unacceptable use across the Trust community.

All individuals accessing Trust-owned or managed digital systems are expected to read, understand, and adhere to this policy. Breaches may result in disciplinary action, withdrawal of access privileges, and/or referral to external authorities where required.

1.B Intended Audience

This Policy applies to all individuals who access or use the Trust's digital systems, devices and information services in a professional capacity. This includes:

- Permanent and temporary staff
- Supply and agency staff
- Visitors and any other individuals granted temporary or ongoing access to Trust IT systems or devices
- Third party contractors
- Governors and trustees

1.C Policy Ownership and Review Cycle

This Policy is maintained by the Trust's **IT Service Delivery Manager** and reviewed by the Trusts **IT Director**, who are responsible for drafting, updating, and ensuring the accuracy and relevance of its content. Oversight and final approval rest with the Trust Board.

The Policy will be formally reviewed on an annual basis, or earlier if required by changes to legislation, statutory guidance, regulatory requirements, or significant changes to technology or operational practice. Interim amendments may be made where necessary to address emerging risks or operational needs.

A revision history will be maintained to document all amendments and updates to this Policy.

2. Legal and Regulatory Framework

This Policy is informed by the following key legislation, statutory guidance, and regulatory requirements. The Trust is committed to ensuring all use of its digital systems, data, and information technologies complies with the following:

- **Data Protection Act 2018** and **UK General Data Protection Regulation (UK GDPR)** – requirements for the lawful processing, protection, and retention of personal data. https://www.legislation.gov.uk/ukpga/2018/12/contents/
- **Computer Misuse Act 1990** – criminal offences relating to unauthorised access to, or misuse of, computer systems and data. https://www.legislation.gov.uk/ukpga/1990/18/contents
- **Human Rights Act 1998** – obligations to respect the privacy and rights of individuals. https://www.legislation.gov.uk/ukpga/1998/42/contents
- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** – provisions allowing lawful monitoring and recording of communications for legitimate business purposes. https://www.legislation.gov.uk/uksi/2000/2699/contents/made
- **Education Act 2011** and **The Education and Inspections Act 2006** – powers relating to searching, screening, and confiscation of devices and material from pupils and others. https://www.legislation.gov.uk/ukpga/2011/21/contents https://www.legislation.gov.uk/ukpga/2006/40/contents
- **Freedom of Information Act 2000** – rights of access to recorded information held by public authorities. https://www.legislation.gov.uk/ukpga/2000/36/contents
- **Keeping Children Safe in Education (KCSIE 2024)** – statutory safeguarding guidance applicable to all schools and colleges in England. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- **Searching, Screening and Confiscation: Advice for Schools (2024)** – guidance to support schools in exercising powers to search and confiscate items. https://www.gov.uk/government/publications/searching-screening-and-confiscation
- **Meeting Digital and Technology Standards in Schools and Colleges (DfE)** – guidance setting out the digital and cyber security standards expected of schools and colleges. https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges#:~:text=All%20schools%20and%20colleges%20must,staff%20responsibilities

All users must comply with the principles and obligations set out in these laws and guidance documents when accessing or using Trust-provided devices, networks, information systems, and services. Breaches of this legal and regulatory framework may result in disciplinary action, referral to law enforcement agencies, or other legal consequences.

The Trust also reserves the right to update this Policy to reflect changes to legislation or regulatory expectations at any time.

3. Roles and Responsibilities

The following section outlines the specific roles, responsibilities, and expectations assigned to individuals and groups subject to this Policy. It defines the accountability and duties of those who use, manage, or oversee the Trust's digital systems, devices, data, and information services, ensuring clarity of purpose and compliance with the legal, regulatory, and operational standards set by the Trust.

3.A The Trust Board

- Ensures overall compliance with legal and regulatory requirements.
- Approves the Acceptable Use Policy and any subsequent amendments.

3.B IT Director and IT Service Delivery Manager

- Own and maintain the Acceptable Use Policy.
- Monitor compliance with this Policy and investigate any breaches.
- Ensure systems, devices, and data are protected in line with legislation and Trust standards.
- Provide training and guidance to users as required.

3.C Designated Safeguarding Lead (DSL)

- Act as the primary contact for online safeguarding concerns.
- Liaise with external safeguarding agencies where required.
- Ensure that online safety is embedded within safeguarding processes.

3.D Staff, Governors, Supply Staff, and Volunteers

- Read, understand, and comply with this Policy.
- Use Trust-provided systems, devices, and information responsibly and lawfully.
- Report any actual or suspected breaches of this Policy immediately to the IT Director or IT Service Delivery Manager.
- Take reasonable steps to protect devices and data from unauthorised access, loss, or damage.
- Maintain the confidentiality of information in accordance with GDPR and the Data Protection Act 2018.

3.E Third-Party Contractors and Service Providers (where applicable)

- Comply with this Policy as a condition of working with or on behalf of the Trust.
- Ensure their staff and representatives follow the same expectations when accessing Trust systems or data.

3.F Data Protection Officer (DPO)

The Trust's Data Protection Officer (DPO) is responsible for advising on, and monitoring compliance with, the UK GDPR and Data Protection Act 2018. The DPO acts as a contact point for data subjects and regulatory authorities and oversees the Trust's data protection obligations. Staff must cooperate

with the DPO in matters of data protection compliance.
Details of the current DPO are set out in the BCWCAT Data Protection Policy[1]

References

1. BCWCAT (2025) *Data Protection Policy, "*Section 5.2 p.7" [online] Available at: https://bcwcat.co.uk/Policies/ (Accessed: 8 May 2025)

4. Acceptable Use Expectations

All individuals covered by this Policy are expected to use the Trust's digital systems, networks, devices, and information responsibly, ethically, and lawfully. The following expectations apply to all users, including the use of personal devices as permitted under Section 5 (Use of Personal Devices - BYOD).

4.A General Expectations

- Use Trust systems, devices, and services only for legitimate Trust-related work and activities.
- Take all reasonable steps to protect devices, accounts, and data from unauthorised access, loss, or damage.
- Handle personal data and confidential information securely and in accordance with the Data Protection Act 2018 and UK GDPR.
- Staff must actively promote safe and responsible use of technology and online behaviour by students, in line with safeguarding policies and Keeping Children Safe in Education (KCSIE 2024). Staff should model positive digital behaviours and reinforce safe online practices in their day-to-day work with students.
- Report any suspected data breaches, system misuse, or cybersecurity incidents immediately to the Trusts IT Management Team.

4.B Use of Accounts and Passwords

- Users are responsible for all activity carried out under their account credentials.
- Passwords must be kept confidential and must not be shared, written down on paper, or stored electronically where they can be publicly viewed.
- Passwords must be a minimum of 8 characters, contain a mix of letters, numbers and special characters, and must not use easily guessed information, common words, or predictable patterns.
- Users must ensure their Trust accounts are secured using multi-factor authentication (where available) and must not disable or bypass this security feature.

4.C Use of Personal Email Accounts

Users **must not** use personal email accounts (e.g., Gmail, Outlook, Yahoo) to access, send, or store any Trust-related information or to log in to Trust systems and services.

- All work-related communication must be conducted using Trust-provided email accounts.
- Trust systems must only be accessed using official Trust credentials and communication channels.
- Using personal email for Trust business poses significant data protection, safeguarding, and cyber security risks and is strictly prohibited.

4.D Email and Communication

- Only use Trust-provided email accounts and communication tools for Trust business.

- Personal email addresses must not be used to send or receive work-related information.
- Do not send offensive, discriminatory, defamatory, or inappropriate material via any communication platform, unless it is necessary and appropriate to report an incident in a professional and factual manner.
- 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 subject to disclosure under the Data Protection Act 2018 or as part of legal proceedings.
- Attachments containing sensitive or confidential information must be encrypted and sent securely.
- If an email containing personal data is sent in error, it must be reported immediately to the Trusts IT Management and the Data Breach Procedure followed.
- Do not engage in bullying, harassment, or intimidation through digital communication.

4.E Internet and System Access

- Do not attempt to bypass security controls, monitoring systems, or web content filters.
- Do not access, store, or share inappropriate, illegal, or offensive material.
- Do not download or install unauthorised software on Trust or personal devices used to access Trust systems.
- Do not attempt to gain unauthorised access to restricted areas, accounts, or password-protected systems.
- Do not create, install, or use any program or tool with the intent to interfere with or disrupt Trust ICT systems or data.

4.F Social Media and Public Communications

- Ensure that personal use of social media does not interfere with work responsibilities.
- Do not use social media in a way that brings the Trust into disrepute or compromises safeguarding or confidentiality.
- Users must respect intellectual property and copyright laws when creating, sharing, or publishing materials online.
- Staff must not publish or share images, videos, or personal information of pupils or colleagues on any platform without prior consent and in accordance with the Trust's safeguarding and data protection policies.
- Where images are used for authorised school purposes (e.g. on the school website), individuals must not be identified by full name or other personal details. For pupils, consent must be obtained in line with the Trust's pupil image consent procedures. Where possible, staff should use only the individual's first initial and surname to further minimise personal data exposure.

- Staff must act as positive role models and always maintain professionalism when posting or commenting online, including on personal accounts.
- Any concerns about inappropriate online behaviour, breaches, or safeguarding risks must be reported immediately to the Designated Safeguarding Lead (DSL) or IT Director.

4.G Device Use and Security

- Do not leave Trust devices (or personal devices used for work) unattended and unlocked in insecure locations.
- Follow Trust guidance for the safe use of Trust and personal devices, as outlined in Section 5.
- Report loss or theft of any device used to access Trust systems immediately.
- Staff must not provide their personal phone numbers to students, parents, or external contacts for work-related purposes.
- All work-related calls must be made using the Trust's telephone system or the staff member's allocated 3CX work extension.
- School or Trust phones, including 3CX systems, must not be used for personal matters.
- Staff issued with mobile phones or telephony equipment for their role must comply with the same standards of use as apply to all other Trust ICT devices and services.

4.H Compliance

- All users must comply with this Policy, related Trust policies, and any reasonable instructions issued by the IT Director, IT Management, or Trust leadership.

Failure to comply with these expectations may result in disciplinary action, withdrawal of access to systems, and/or referral to external agencies, including law enforcement, where applicable.

5. Use of Personal Devices (BYOD)

The Trust permits the use of personal devices (such as smartphones, tablets, and laptops) to access Trust systems and services for work purposes, subject to the following conditions:

5.A General Expectations

- Personal devices may only be used to access Trust-approved services, such as email, Teams, and approved cloud platforms.
- Users must take all reasonable steps to protect Trust data accessed or stored on personal devices, including the use of device passcodes, encryption where available, and up-to-date antivirus protection.
- Personal devices must not be used to store large volumes of Trust data or special category (sensitive) personal data.

5.B Security and Compliance

- The Trust may require personal devices used for work to be enrolled in mobile device management (MDM) or equivalent security measures, where appropriate.
- Users must report the loss, theft, or suspected compromise of any personal device used to access Trust data immediately to the IT Director or IT Management.
- Personal devices must not be used to circumvent security controls or content filtering applied to Trust-owned devices and networks.
- Users are responsible for ensuring that personal devices are regularly updated with security patches and operating system updates.

5.C Acceptable Use

- The use of personal devices must not interfere with the performance of work duties or breach any provisions of this or any other Trust policy.
- The Trust reserves the right to withdraw BYOD access at any time if security or compliance risks are identified.

Use of personal devices to access Trust systems constitutes acceptance of these conditions. Failure to comply may result in withdrawal of access to Trust systems and/or disciplinary action.

6. Monitoring and Filtering

The Trust reserves the right to monitor, access, and review any use of its digital systems, devices, services, and networks, including activity conducted on personal devices where such activity passes through Trust-controlled systems, as outlined in Section 5. This is to ensure the security, integrity, and appropriate use of Trust resources, safeguard users, and comply with legal and regulatory obligations[1].

6.A Purpose of Monitoring

Monitoring may be conducted for purposes including, but not limited to:

- Protecting the safety and welfare of staff and pupils in line with Keeping Children Safe in Education 2024[1,2]
- Ensuring compliance with the Trust's policies and legal obligations[4]
- Preventing, detecting, and investigating misuse or cybersecurity incidents[4]
- Maintaining the operational integrity of Trust systems and infrastructure

6.B Methods of Monitoring

The Trust uses a range of tools and methods to monitor and filter activity, including:

- Web filtering and content monitoring systems, including Smoothwall and Senso
- Network traffic analysis and firewall logs
- Email and communication scanning for policy breaches or safeguarding risks
- Device activity logging and audit trails on Trust-managed devices
- CCTV coverage in areas where applicable[3]

6.C User Awareness and Consent

By accessing and using Trust systems, services, or networks, users acknowledge and consent to such monitoring as a condition of use. Monitoring will be conducted proportionately and lawfully, with appropriate regard to privacy and data protection legislation.[4]

6.D Personal Devices

The Trust does not install monitoring software or management tools on personal devices.[4] However, any activity conducted using personal devices to access Trust systems, services, or data, or any use of personal devices connected to the Trust's staff or guest Wi-Fi networks, may be logged and monitored through the Trust's network security systems, including but not limited to firewall logs, web filtering, and safeguarding platforms such as Smoothwall and Senso. Use of personal devices on Trust networks constitutes acceptance of these conditions.

Failure to comply with this Policy may result in disciplinary action, withdrawal of access rights, and/or referral to law enforcement agencies or regulatory bodies as required.

References

1. Department for Education. (2024*) Keeping children safe in education: Statutory guidance for schools and colleges*, "p. 39, 137." [online] Available at: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 [Accessed 8 May 2025].
2. Ibid., "p. 39, 140.".
3. Ibid., "p. 93, 369."
4. HM Government (2000) *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,* "Regulation 3" [online] Available at: https://www.legislation.gov.uk/uksi/2000/2699/contents/made

Appendix 1 – BCWCAT Staff Acceptable Use Agreement (AUA)

BCWCAT Trust Staff Acceptable Use Agreement 2025

This agreement forms part of the BCWCAT Acceptable Use Policy (AUP) for staff, governors, supply staff, and volunteers. By signing this agreement, you confirm that you have read, understood, and agree to abide by the full BCWCAT Acceptable Use Policy.

Important:

The full BCWCAT Staff Acceptable Use Policy (AUP) can be accessed online at https://bcwcat.co.uk/Staff-Policies/.
This agreement must not be signed unless the full BCWCAT Staff Acceptable Use Policy has been read and understood.

As a staff member, governor, supply staff, or volunteer I agree that:

General use

- I will use Trust systems, devices, and services responsibly, ethically, and lawfully in line with the AUP.
- I understand that the Trust will monitor my use of digital technology and communications systems as outlined in the AUP.
- I understand that these rules apply both on and off-site when using Trust devices, systems, or data, or when using personal devices for Trust work.
- I will not share my login credentials, and I will protect all accounts with a secure password and multi-factor authentication where required.
- I will immediately report any illegal, inappropriate, or harmful material or incidents to the Designated Safeguarding Lead (DSL)

Professional conduct

- I will communicate professionally and respectfully when using Trust systems.
- I will not use personal email or messaging apps to communicate with pupils or parents/carers.
- I will not attempt to access, copy, modify, or delete any other user's files without permission.
- I will only publish or share images of pupils or staff where prior consent has been obtained and in line with the Trust's safeguarding and data protection policies.
- Where possible, I will avoid identifying individuals by their full names in published materials and will use minimal or partial name formats.
- I will not post or comment on social media in a way that could compromise my professional responsibilities or bring the Trust into disrepute.

- I will not use my personal phone number to contact pupils or parents/carers and will only use my allocated 3CX extension or Trust-provided device.
- I will not engage in any activity that could compromise data protection, online safety, or safeguarding expectations.

Device and system use

- I will follow Trust guidance for any personal devices used for Trust work (BYOD) and ensure they are secure, updated, and protected by appropriate security controls.
- I will ensure that data containing personal information is securely stored and encrypted where required.
- I will not attempt to bypass Trust security controls, install unauthorised software, or interfere with Trust systems.
- I will not use Trust systems to engage in any illegal, offensive, or inappropriate activity.
- I understand that any breach of system security or data protection must be reported immediately.

Compliance and responsibility

- I will comply with all relevant Trust policies, including the Data Protection Policy and Online Safety Policy.
- I will respect copyright and intellectual property rights when using and sharing digital materials.
- I understand I am responsible for my professional conduct both inside and outside of the workplace where it relates to the Trust.
- I understand that failure to comply with the AUP may lead to disciplinary action, withdrawal of access, referral to the Trust Board, or involvement of external agencies including the police where appropriate.

Declaration

I confirm that I have read, understood, and agree to comply with the BCWCAT Staff Acceptable Use Policy and this Staff Acceptable Use Agreement. I understand my responsibilities and the potential consequences of failing to follow this agreement.

Name (print): _____

Role: _____

Signature: _____

Date: _____

Appendix 2 – Key Definitions

AUP – Acceptable use policy the rules and expectations for safe and responsible use of Trust ICT systems and data

BYOD – Bring Your Own Device: staff use of personal devices (e.g. mobile phones, laptops) for work purposes under Trust conditions.

DPO – Data Protection Officer: responsible for overseeing compliance with data protection legislation and handling data-related enquiries.

DSL – Designated Safeguarding Lead: staff member with lead responsibility for safeguarding and child protection in a school.

ICT – Information and Communication Technology.

MFA – Multi-Factor Authentication: a security method requiring two or more forms of verification to access systems or accounts.

IT Management Team

Name	Role	Email	Telephone
Christopher Jakubowski	IT Director	chris.jakubowski@bcwcat.co.uk	01274941946
Josef Bodnarczuk	IT Service Delivery Manager	jbodnarczuk@sbsj.co.uk	01274941948
Chris Domenech	Network operations Manager	cdomenech@holyfamilyschool.uk	01535612826

Version Control

Status	Version	Date	Author
Final	v0.1	11/05/2025	Josef Bodnarczuk (ITSDM)
Pending Approval	V1.0	15/05/2025	