Barnet Special Education Trust

Title	BSET-Pol.49-Staff and Third Party BYOD Policy
Executive Owner	Lynda Walker (CEO)
Effective Date	01/07/2025; 30/06/2026
Review Date:	30/06/2027
Related Policies	Information Security Policy, Data Protection Policy
Related committee for review	Board of Trustees
Approved at meeting BOT	20/07/2026
Filed as	BSET-Pol.49_Staff and Third Party BYOD Policy_V2.1

Version Information & Changes

Any changes, edits and updates made to the Staff and Third-Party BYOD Policy will be made in here. It is the responsibility of the Central Business Team to ensure that all existing copies of this policy are up to date. Whenever there is an update to this policy, this document requires that the version number be updated to reflect the changes.

Name of person making change	Role of person making change	Date of change	Version number	Notes
Gayan Fernando	Head of IT	10/02/2025	1.0	First draft of the BYOD Policy
Gayan Fernando	Head of IT	25/03/2025	1.1	Monitoring and Access section added
Annie Dobbin	HR Manager	04/06/2026	2	improves clarity, legal protection, and operational guidance by adding detailed sections on liability, privacy, reporting, and offboarding.
Annie Dobbin	HR Manager	20/07/2026	2.1	References Smart watches/glasses

1. Rationale

BYOD (Bring Your Own Device) is a concept of authorised users using their personally owned device(s) to access Trust Information Assets (TIAs). These devices are subject to the equivalent minimum baseline security requirements as corporately owned and provided devices. BYOD must be included within our Cyber Essentials scope.

2. Purpose

The Trust, Cyber Essentials and the UK GDPR have identified a set of minimum baseline security requirements and good practice guidance to provide assurance against cyber-attacks and data breaches.

3. Scope

Personally owned devices that access TIAs include but are not limited to:

- Computer and Laptops
- Phones and Tablets
- Smart watches and glasses
- Devices owned by trusted third parties

This policy does not apply to students.

4. Policy

Device Enrolment

The following links will help guide enrolment of personally owned devices. Successful enrolment and ongoing access to TIAs is conditional on meeting compliance requirements. Some requirements are technically evaluated whilst others must be adhered to by complying with this policy.

- Windows 10/11
- macOS
- iOS
- Android
- Linux

Enrolment will allow the Trust to view some information on your personally owned device. For further information, please see here.

Some limited configuration changes will be made to your personally owned device to support access to the Trust network. These include:

- Installation of certificate files and configuration of your device's network settings to support authentication when connected to the Trust network.
- Disabling MAC randomisation (currently limited to iOS) when the device is used to connect to the wireless network.

These settings are removed if you choose to unenroll your device. For further information, please see here.

For technical reasons, some online services provided by the Trust may remain accessible from unenrolled devices. In these scenarios, users must ensure that their device is enrolled and that all the following requirements are met before access is attempted.

Software

- Operating systems, firmware and applications must be fully supported by the vendor, haver the latest security patches installed, and set to auto-update wherever possible.
- Software and services no longer used must be removed/disabled prior to enrolment.
- Devices should be regularly rebooted to allow the installation of updates.

Accounts

- Do not use generic/shared accounts and do not share single account devices, i.e, do not allow others to share your computer or laptop account or share your enrolled mobile phone or tablet.
- For computers and laptops:
  - Users must set up a separate user account profile without Administrative or Elevated privileges on their device for the purpose of accessing Trust data on devices. This may require creating a new profile for Trust use. For further information, please see here for Windows and here for macOS.
  - Separate administrator accounts must only be used for privileged activities such as installing software or making configuration changes. For the avoidance of doubt, administrator accounts must not be used.
  - The Trust reserves the right to restrict access for devices deemed to be detrimental to the security or operation of its systems.

Passwords

- The password that is assigned to any account or device (i.e. default password) must be changed immediately.
- Standard user accounts must be a minimum of eight characters and difficult to guess (a minimum of twelve characters is required for administrator accounts). Passwords must include at least some or all the following: uppercase letters, numbers, and special characters, and not use words that can be easily attributed to you or easily found out such as children's names, pet names, favourite football team, etc.
- Even longer passwords are encouraged which can be created by stringing together three random words, or alternatively, by automatically generating and storing them in a password manager (e.g. KeePass, which is freely available).
- Unique passwords must be used for every account and not written down.
- Passwords must be changed if believed to be compromised. Trust accounts can be reset on the Self Service Password Portal.
- Auto-run and auto-play must be disabled. For further information, please see here for Windows and here for macOS.

Anti-malware

- For non-iOS devices, anti-malware software must be installed and configured in accordance with the vendor's best practice guidance. Microsoft Defender is sufficient for Windows devices, but for other platforms, it is recommended to install anti-malware software that receives top marks through an independent validation process.
- Ant-malware software must be configured to update at least daily and to scan files automatically upon access.
- Anti-malware software must be configured to scan web pages and warn upon access to malicious websites.

Approved Software

- An approved software list is published on the Company Portal for non-Trust owned devices, and only this software, including web browsers, may be used to access TIAs.
- Mobile apps must only be installed from the vendor's app store
- Mobile devices must not be jailbroken or rooted or support sideloading.

Device locking

- Reauthentication is required after a device has been idle for 10 minutes.
- Computers and laptops must require username/password authentication when first logged on, or else use a 6-character PIN, fingerprint, or face ID

Encryption

- To comply with the Trust's IT Security Policy and to support GDPR, as an appropriate measure to ensure that personal data is processed securely, device encryption must be enabled

Device Loss or Unauthorised Access

- Users shall report loss of, or unauthorised access to, a personal device which has been used to access Trust data without delay and will co-operate in wiping Trust information from the device wherever possible and reasonable
- Any misuse, or suspected misuse of a device or breach of this policy will be dealt with in accordance with the Trust ICT and Internet Acceptable Use Policy

5. Responsibilities

Authorised Users	- Ensure that personally owned devices align to this policy before using them to access TIAs - Manage and remediate personally owned devices such that all requirements in this policy continue to be met.
Authorised Reviewer	- Review this document, summarise any resulting changes and

	improvements, and create minor revisions.
Document Owner	- Maintain this document - Assure the quality of any changes - Create major revisions following document approval
Approver	- Understand the organisational implications of this document and support its contents

6. Monitoring and Access

The Trust will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks.
- Activate remote wipe facility, if the device is reported missing or unauthorized access is detected.
- Install relevant "Company Apps", which will enable users to access TIAs.

7. Compliance

The Staff and Third-Party BYOD Policy shall be enforced to meet specific compliance requirements, including but not limited to:

- BSET ICT and internet acceptable use policy
- Cyber Essentials
- General Data Protection Regulation
- BSET Information Security Policy
- UK Data Protection Act 2018

Section 8: Liability and Responsibility

8.1 Device Ownership and Liability

- Personal devices used under this BYOD policy remain the sole property of the individual user.
- The Trust accepts no responsibility or liability for any damage to, loss of, or theft of personal devices, whether the device is on Trust premises or being used to access Trust Information Assets remotely.
- Users are responsible for ensuring their personal devices are adequately insured. The Trust strongly recommends that users check their personal insurance policies to ensure coverage extends to use of devices for work purposes.

8.2 Repair and Replacement Costs

- All costs associated with the repair, replacement, or maintenance of personal devices are the sole responsibility of the device owner.
- The Trust will not provide financial compensation or reimbursement for any damage, loss, or theft of personal devices, regardless of the circumstances.

8.3 Data Charges and Connectivity

- Users are responsible for any data charges, roaming fees, or connectivity costs incurred when using personal devices to access Trust Information Assets.
- The Trust will not reimburse users for mobile data usage or internet connectivity costs associated with BYOD.

8.4 Malware and Security Incidents

- While the Trust requires anti-malware software to be installed on personal devices (as per Section 4), users remain responsible for maintaining the security of their devices.
- The Trust is not liable for any security breaches, malware infections, or data loss that may occur on personal devices, even when accessing Trust systems.

Section 9: Privacy and Data Access

9.1 Information the Trust Can Access

When you enrol your personal device to access Trust Information Assets, the Trust may be able to view the following information:

For all devices:

- Device name and model
- Operating system version
- Installed security updates
- Compliance status with this policy
- Network connection information
- Installed applications list (limited to verification of approved software)

The Trust will NOT access:

- Personal files, photos, videos, or documents stored on your device
- Personal emails, text messages, or call logs
- Browsing history outside of Trust systems
- Location data (except where required for device security if reported lost/stolen)
- Personal app data or content

9.2 How Information is Used

Information collected from enrolled devices will be used solely for:

- Verifying compliance with security requirements
- Protecting Trust Information Assets
- Responding to security incidents
- Managing access to Trust systems

9.3 Data Retention

- Device information will be retained only for as long as the device remains enrolled and you are employed by/working with the Trust.
- Upon unenrolment or termination of your relationship with the Trust, device information will be deleted in accordance with the Trust's Data Protection Policy.

9.4 Your Rights

Under UK GDPR, you have the right to:

- Request access to the information the Trust holds about your device
- Request correction of inaccurate information
- Request deletion of your device information (subject to legitimate Trust interests)

To exercise these rights, contact the Trust's Data Protection Officer via Satswana.

Section 10: Policy Breach Reporting and Consequences

10.1 Reporting a Policy Breach

If you become aware of a breach of this policy (by yourself or others), you must report it immediately.

How to report:

- For technical issues or security concerns: Contact the IT Helpdesk at Interm IT
- For policy violations: Contact your line manager.
- For serious concerns about data breaches: Contact the Data Protection Officer immediately at Satswana

Timescales:

- Security incidents (e.g., suspected malware, unauthorised access): Report immediately upon discovery
- Lost or stolen devices: Report within 2 hours of discovery
- Other policy breaches: Report within 24 hours of discovery

10.2 What to Include in Your Report

When reporting a breach, provide:

- Your name and contact details
- Date and time the breach occurred or was discovered
- Description of what happened
- Which device(s) are affected
- What Trust data may have been compromised (if applicable)
- Any steps you have already taken

10.3 Consequences of Non-Compliance

Failure to comply with this policy may result in:

Immediate actions:

- Suspension of access to Trust systems and data
- Removal of device from the Trust network
- Investigation in accordance with the Trust's disciplinary procedures

Potential outcomes:

- For minor or first-time breaches: Additional training and monitoring
- For repeated or serious breaches: Formal disciplinary action in accordance with the Trust's Disciplinary Policy, which may include dismissal
- For breaches involving data protection violations: Referral to the Information Commissioner's Office (ICO) where required by law
- For third-party contractors: Termination of contract

10.4 Support and Training

The Trust recognises that some policy breaches may occur due to lack of understanding rather than intentional misconduct. Where appropriate, the Trust will provide:

- Additional training on security requirements
- Technical support to help users meet compliance standards
- Clear guidance on how to prevent future breaches

Section 11: Staff Consultation and Communication

11.1 Policy Development

This policy has been developed in consultation with:

- Trust IT staff and security specialists
- Heads of Provision and trustees

11.2 Communication of Policy

All staff and third parties who may use personal devices to access Trust Information Assets will be informed of this policy through:

- Induction processes for new staff
- Email notification when the policy is updated
- Publication on the Trust intranet/staff portal

11.3 Requesting a Copy

A copy of this policy is available:

- On the Trust website at Barnet Special Education Trust - Policies
- On the staff intranet / Staff sharepoints

11.4 Accessibility

The Trust is committed to ensuring this policy is accessible to all staff. If you require this policy in an alternative format (e.g., large print, audio, Braille), please contact [insert contact details].

Section 12: Leaving Employment or Ending Third-Party Relationships

12.1 Unenrolment Process

When your employment or contract with the Trust ends, you must:

- Immediately cease accessing Trust Information Assets from your personal device
- Contact the IT Helpdesk to arrange unenrolment of your device
- Delete all Trust data from your personal device
- Return any Trust-issued certificates or credentials

12.2 What Happens to Your Device

Upon unenrolment:

- Trust-specific settings and certificates will be removed from your device
- Your access to Trust systems will be revoked
- The Trust will delete information about your device from its systems
- Your personal data and files will remain unaffected

12.3 Trust's Right to Remote Wipe

In accordance with Section 6, if you fail to unenrol your device or return Trust data when required, the Trust reserves the right to remotely wipe Trust information from your device. This will only affect Trust data and should not affect your personal information, but the Trust cannot guarantee this in all circumstances.