Policy

Bring Your Own Device (BYOD)

May 2025

Bring Your Own Device (BYOD)

1. Purpose

This policy outlines the responsibilities and security requirements for trustees, staff and volunteers using personal devices (e.g., smartphones, tablets, laptops) to access the organisation's systems, data, and resources. It also includes guidelines on consent, risk mitigation, and actions for non-compliance.

2. Scope

This policy applies to all trustees, staff and volunteers who use their personal devices to access company email, files, software applications, or other work-related systems. In some instances, trustees, staff and volunteers may be required to use their personal devices for specific work-related purposes, such as multi-factor authentication (MFA).

3. Policy Principles

The organisation permits trustees, staff and volunteers to use personal devices for work-related activities, provided they comply with the security, privacy, and consent requirements outlined in this policy.

4. Consent and Data Privacy

4.1. Consent to BYOD Policy Terms

- Before using personal devices for work, trustees, staff and volunteers must provide explicit consent to adhere to Wheels for All's BYOD and GDPR policies, particularly where the organisation may require personal devices for specific work functions (e.g., MFA).
- Consent must be captured in writing or via a secure electronic form that acknowledges:
    - The organisation's right to monitor work-related activities on personal devices.
    - The requirement to use personal devices for specific functions, such as MFA.
    - The organisation's ability to remotely wipe work-related data if a device is lost, stolen, or if there is a data breach.
    - Compliance with the security measures outlined in this policy.
- Consent will be collected by the Operations and Administration Officer
- Consent will be renewed as policy changes deem necessary.

4.2. Privacy Considerations

- The organisation will take all necessary steps to ensure that personal data (e.g., contacts, photos) on staff's devices is not accessed unless required for work-related compliance or by law.
- Only work-related data and activities will be monitored, and the organisation will not interfere with or monitor personal use of devices outside the work environment.

4.3. Withdrawing Consent

- Trustees, staff and volunteers may withdraw consent at any time, in which case the organisation will remove all work-related access and data from the device.
- Withdrawal of consent may impact the trustee, staff or volunteer's ability to perform certain work-related tasks remotely or access systems that require MFA.

5. Security Requirements

To ensure organisational data security, trustees, staff and volunteers using personal devices must comply with the following requirements:

5.1. Device Security

- All personal devices used for work purposes, including MFA, must be secured with a strong password, PIN, or biometric authentication (e.g., fingerprint, facial recognition).
- Devices must have up-to-date operating systems and security patches installed to protect against vulnerabilities.
- Antivirus software must be installed on personal devices and kept updated.
- Trustees, staff and volunteers using personal devices will be responsible for regularly checking for and installing system updates to maintain both system performance and device security.

5.2. Encryption and Secure Access

- Any device used to access or store work-related information must have full-disk encryption enabled to protect sensitive data.
- Remote access to organisational systems must occur via secure methods, such as a Virtual Private Network (VPN) or Multi-Factor Authentication (MFA).

5.3. Data Storage and Backup

- Work-related data on personal devices must be regularly backed up to an encrypted, secure location approved by the organisation.
- Trustees, staff and volunteers must not store sensitive or confidential organisational data on unsecured cloud services or unauthorised platforms.

5.4. Lost or Stolen Devices

- In the event a personal device is lost or stolen, trustees, staff and volunteers must report the incident immediately to management@wheelsforall.org.uk and their line manager.
- The organisation reserves the right to remotely wipe work-related data from the personal device in the event of loss, theft, or security breach.

6. Risk Mitigation

6.1. Device Loss or Theft

- In the event of a lost or stolen device, trustees, staff and volunteers must immediately report it to management@wheelsforall.org.uk and their line manager.
- The organisation reserves the right to remotely wipe work-related data to prevent potential data breaches.

6.2. Security Breach

- If a security breach occurs on a personal device, the organisation will initiate a remote data wipe for work-related information to mitigate risks.
- Trustees, staff and volunteers must cooperate fully with the organisation during any investigations of data breaches or security concerns.

6.3. Mitigation Strategies

- Regular security training will be provided to all trustees, staff and volunteers to ensure awareness of best practices for handling work-related data on personal devices.
- Periodic device audits may be conducted to verify compliance with the BYOD security requirements.

7. Non-Compliance

7.1. Refusal to Comply

- If a trustee, staff or volunteer does not agree to the terms of this policy, they will not be permitted to use their personal device for work purposes. Alternative arrangements may be considered.

7.2. Non-Compliance Actions

- Non-compliance with the security measures outlined in this policy (e.g., failing to install latest security patches or using an unencrypted device) will result in the revocation of access to work-related systems from the personal device.
- Repeated non-compliance or refusal to adhere to the policy will result in disciplinary actions as per the organisation's policies.

7.3. Inability to Perform Duties

- Trustees, staff and volunteers who choose not to comply with the BYOD policy and cannot perform key duties as a result will need to discuss alternative solutions with their manager. This could include reassignment of tasks or provision of alternative equipment.

8. Acceptable Use

8.1. Use of Personal Devices

- Personal devices must not be used to access or store illegal or inappropriate material while being used for work-related purposes.

8.2. Monitoring and Oversight

- The organisation reserves the right to monitor work-related activity on personal devices, including access to company emails, files, and applications.

9. Support and Liability

9.1. IT Support

- The organisation will provide limited IT support for setting up and maintaining secure access to work systems on personal devices, particularly for MFA or secure remote access.
- For support to access to work systems on personal devices, please contact support@hudsonhill.co.uk

9.2. Liability

- Staff are responsible for any repair, maintenance, or replacement costs associated with their personal devices.
- The organisation is not liable for any personal data loss or damage caused by work-related applications or remote data wiping.

10. Termination of Employment

- Upon termination of employment, the organisation will remove all work-related data and access from personal devices.
- All organisation-owned equipment or software used for accessing work systems on personal devices must be returned.

11. Review of Policy

This policy will be reviewed annually to ensure it remains up to date with technological advancements and security best practices.

12. Document Control and Approval

The COO is the owner of this document and is responsible for ensuring that this procedure is reviewed regularly.
A current version of this document is available to all members of staff and is the published version.

Version Information

Version	Date	Author(s)	Details
1.0	09/05/2025	Joe McTague	Approved