Policy

User IT Policy

May 2025

User IT Policy

Table Contents

User IT Policy

1. Acceptable User Policy

1.1. Introduction

The purpose of this policy is to outline the acceptable use and security requirements for information technology (IT) resources at Wheels for All. This policy ensures that all users understand their responsibilities to protect the organisation's data, systems, and services. It supports the organisation's compliance with relevant legislation and best practices.

- Information security protects against accidental or malicious disclosure, modification, or destruction.
- Information is an important & valuable organisation asset, which must be managed with care and all information has a value to our organisation, trusted partners or criminal actors.
- Access controls regulate who can use information resources and ensure proper procedures for granting and changing access as appropriate to your role.
- Password creation and protection are mandated, supported by two-factor authentication (2FA).

1.2. Definition, Purpose, Scope, and Risk

1.2.1. Definition of this policy covers access control rules and procedures required to regulate who can access information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing organisations information in any format and on any device

1.2.2. Purpose of this policy aims to prevent unauthorised access. The policy describes the registration and de-registration process for all organisation information, systems and services, especially for new starters, leavers, and role changes.

1.2.3. Scope applies to all information, systems, networks, applications, locations, and users (staff, volunteers, trustees, and partners). This includes hardware such as laptops and mobile devices.

1.2.4. Risk is that on occasion, organisation information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies,

without the correct authorisation and clearance, may intentionally or accidentally gain unauthorised access to our information which may adversely affect day to day operations. This policy is intended to mitigate that risk.

1.2.5. Additional risk is that non-compliance with this policy could have a significant effect on the efficient operation of our organisation and may result in financial and/or reputational loss and an inability to provide necessary services to our customers.

1.3. Internet Use

1.3.1. Wheels for All internet access is for business purposes, including research, communication with partners, and operational efficiency.

1.3.2. Personal use should be minimal and must not interfere with work responsibilities.

1.3.3. Access to websites containing obscene, hateful, or otherwise inappropriate content is strictly prohibited.

1.3.4. Users must not bypass security controls, introduce malware, or engage in activities that compromise cybersecurity.

1.3.5. Any software or downloads must be approved by IT support before installation.

1.3.6. Users must avoid sharing confidential information on public forums, including social media, without prior authorisation.

1.3.7. Users must not access or download inappropriate, offensive, or sexually explicit material. Any attempt to do so may constitute gross misconduct.

1.3.8. The downloading of entertainment content, including music or video, is prohibited unless directly related to work duties.

1.3.9. The Charity may block access to websites it considers inappropriate. Regardless of whether a site is blocked, accessing prohibited content is not allowed.

1.4. Usage of Email and Communication Activities

1.4.1. Wheels for All email accounts must be used for official communications. Personal use should be limited and not interfere with business needs.

1.4.2. Users must not send emails containing harassment, discrimination, defamatory content, or personal opinions misrepresented as organisational statements.

1.4.3. Sending inappropriate material (e.g. sexual, racist, or discriminatory content), jokes, chain letters, or unauthorised bulk mail from a charity email address is strictly prohibited and may be treated as gross misconduct.

1.4.4. Users must treat email correspondence with the same professionalism as any other formal communication.

1.4.5. Confidential information must be encrypted and only shared with authorised recipients.

1.4.6. Emails from unknown or suspicious sources should not be opened. If multiple such emails are received, they must be reported to IT support.

1.4.7. Distribution of bulk emails or spam is not permitted unless authorised for organisational communications.

1.4.8. If offensive material is received, it must be reported to management immediately.

1.5. Online Conduct Behaviour

1.5.1. When using Wheels for All accounts, users must act professionally and respectfully in all online communications, including emails, social media, and virtual meetings.

1.5.2. Users must not engage in cyberbullying, harassment, or any form of discriminatory behaviour while using Wheels for All digital resources.

1.5.3. Personal opinions must not be presented as official Wheels for All statements.

1.5.4. Posting or sharing any inappropriate, offensive, or harmful content using Wheels for All accounts is strictly prohibited.

1.5.5. Online collaboration platforms (e.g., Teams, SharePoint) must be used for Wheels For All purposes only and must not be misused for personal or unauthorised activities.

1.5.6. Users should ensure that their online behaviour aligns with Wheels for All's values, maintaining a positive and inclusive environment.

1.6. Compliance and Monitoring

1.6.1. Wheels for All reserves the right to monitor internet and email usage to ensure compliance with this policy.

1.6.2. Any violation of this policy may result in disciplinary action, including access restriction, formal warnings, or termination.

1.6.3. Users are responsible for maintaining the security of their credentials and must not share login details with unauthorised individuals.

1.7. System Security & Appropriate Use

1.7.1. It is vital that Wheels for All keeps its systems and data secure. All users must comply with any instructions issued by management or IT support regarding the use of charity-owned computers, accounts, systems, or devices.

1.7.2. You must not attach any hardware or storage device to any Wheels for All equipment without prior authorisation from your line manager. Similarly, users must not download or install any software, plugins, or extensions unless cleared by management. Anti-virus and firewall protections must not be disabled under any circumstances.

1.7.3. When leaving your workstation for any extended period, users must lock their screen or log off to prevent unauthorised access.

1.7.4. Passwords must be strong, confidential, and regularly updated.

1.7.5. Portable IT devices provided by Wheels for All must be always kept secure and password protected.

1.7.6. Unauthorised access to any of the Charity's systems will be treated as gross misconduct and may result in dismissal.

2. IT Security & Access Management

2.1. Physical Access

Physical Access is every individual's responsibility for any device they are issued or use to access our systems. Individuals are to:

2.1.1. Users must not leave devices unattended in insecure locations.

2.1.2. Access to offices and storage areas must be restricted to authorised personnel only.

2.1.3. Any lost or stolen devices must be reported immediately to IT support or management.

2.1.4. Ensure that the location of device(s) issued to them are always known.

2.1.5. Ensure they follow the organisation's mandatory password access controls for devices.

2.1.6. Prevent access to any organisation's device or data from any person not authorised.

2.1.7. When you are not using the device, you must ensure that the device is locked and any display screen or any other access port available via the device must be made secure from unauthorised viewing or access prior to leaving the device.

2.1.8. Devices may not be left unattended in the office at any time when there is no organisation staff present.

2.1.9. Devices that are to be left in the office for an extended period of time or overnight must be shut down to enforce password protection

2.1.10. Access to physical network devices within the organisation's office is restricted.

2.1.11. Access to the network room is controlled by authorised staff member who maintains a register of personnel permitted to access and operates a controlled key process to maintain security.

2.1.12. Any suspected or known unauthorised access to a device must be reported immediately to your line manager.

2.2. Building Access

2.2.1. Physical access to the organisation's office is controlled and administered by key given to authorised staff members. This key must not be shared with anyone without prior authorisation from senior manager.

2.2.2. Only organisation staff will be permitted to apply for a building security key / pass.

2.2.3. Where an individual does not have a key / pass, they will be required to contact office reception or member of the office staff ahead of time.

2.2.4. All guests must be notified to reception to have access to the building and are not permitted to pass the reception area without being escorted by a authorised staff.

2.2.5. Any keys issued must be returned to the line manager on termination of employment.

2.2.6. Cleaning staff are permitted access to offices and communal areas for cleaning only and are instructed to notify office manager of any device found unsecured during their cleaning.

2.3. Passwords

2.3.1. Choosing Passwords

Passwords are the first line of defence for our IT systems and together with the user ID helps to establish that people are who they claim to be.

2.3.1.1. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our information, computers and systems.

2.3.1.2. To assist users we will deploy 'Two-factor authentication' (2FA) as a second line of defence and user identification.

2.3.2. Defining 'weak' and 'strong' passwords

2.3.2.1. A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

2.3.2.2. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

2.3.3. Everyone must use strong passwords with a minimum standard of:

2.3.3.1. At least eight characters.

2.3.3.2. Contain a mix of alpha and numeric, with at least one digit.

2.3.3.3. Is not based on anything, which could be guessed easily by someone or obtained from personal information such as name, telephone number or date of birth.

2.3.4. Storing Passwords

2.3.4.1. The best way to store passwords is by using a password manager (example Bitwarden). This provides a central repository for passwords and promotes good credential management, especially the creation of complex and unique passwords by offering random password generation.

2.3.5. Protecting Passwords

The following guidelines must be adhered to:

2.3.5.1. Never reveal your passwords to anyone.

2.3.5.2. Never write your passwords down or store them where they are open to theft.

2.3.5.3. Never store your passwords in a computer system without encryption.

2.3.5.4. Do not use any part of your username within the password.

2.3.5.5. Do not use the same password to access different systems.

2.3.5.6. Do not use the same password for systems inside and outside of work.

2.3.6. Changing Passwords

2.3.6.1. Default passwords must be changed after first use.

2.3.6.2. If you become aware or suspect that your password has become known to someone else, you must change it immediately and report your concern to line manager.

2.4. Team Member Access

2.4.1. Access rights are assigned based on your role & tasks, with unique logins and passwords for each system.

2.4.2. Elevated access (e.g., admin rights) must be approved by management and reviewed regularly.

2.4.3. User access must be revoked promptly when no longer required, such as when an individual leaves the organisation.

2.5. User Registration

2.5.1. Each user has a unique ID (organisation email) for system access.

2.5.2. Access is suspended on the last working day of a departing employee.

2.6. User Responsibility

It is a user's responsibility to prevent their user ID and password from being used to gain unauthorised access to organisation's systems by:

2.6.1. Following the Password Policy Statements outlined above.

2.6.2. Ensuring that any Laptop or PC or other devices, when left unattended is logged out and locked away in secure place.

2.6.3. Leaving nothing on display that may contain access information such as login names and passwords.

2.6.4. Informing their line manager if their role and access requirements change at any time. The line manager must inform senior member of staff responsible for administrating IT systems.

2.7. Remote Working

2.7.1. Remote access to Wheels for All systems must be via approved devices and secure connections.

2.7.2. Users must ensure that their home networks and devices meet required security standards, such as using antivirus software and secure Wi-Fi passwords.

2.7.3. Confidential data must not be saved locally on personal devices.

2.7.4. Remote access from outside the UK will not be allowed, unless prior pre-authorised in writing obtained from senior manager.

2.8. Network Access

2.8.1. Unauthorised networking devices are prohibited in the office.

2.8.2. Remote access can only be performed by authorised & approved personal

2.9. Software Access

2.9.1. Only licensed and approved software may be installed or used, with untested software requiring senior management approval.

2.9.2. Requests for new software must be submitted to IT support for approval and compatibility assessment.

2.9.3. Users must not alter or disable security features on software or systems.

2.9.4. Employees must not install any software, plugins, or extensions without prior approval.

2.9.5. Entertainment content such as music or video must not be downloaded to charity-owned devices.

3.Document Control and Approval

The Director 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	21/05/2025	Azad Brepotra Cristina Arion	Approved