**THE WHEELS PROJECT LTD**

**31 - 32 Bonville Road**

**Brislington**

**Bristol BS4 5QH**

Registered Charity No: 1081236

|  |
| --- |
| **INFORMATION TECHNOLOGY and ACCEPTABLE USE POLICY** |

1. **Introduction**

This policy outlines the guidelines and regulations governing the use of information technology (I.T.) resources in The Wheels Project. It aims to ensure the effective and responsible utilisation of technology to enhance learning experiences, promote digital literacy, and protect the integrity and security of I.T. infrastructure and data within the educational institution.

1. **Scope**

This policy applies to all students, faculty, staff, and any other individuals granted access to I.T. resources, whether on-campus or remotely.

1. **Purpose of I.T. Resources**
   1. Educational Enhancement: I.T. resources should be utilised to enhance and enrich the teaching and learning process, providing opportunities for innovative and interactive educational experiences.
   2. Research and Development: I.T. resources may be used for research, development, and educational purposes to foster intellectual growth and advancement.
   3. Administrative Efficiency: I.T. resources should also support administrative functions, streamlining processes and communication within The Wheels Project.
2. **Responsible Use of I.T. Resources:**
   1. Users must respect the privacy of others and protect sensitive data from unauthorised access, disclosure, or modification. Personal data handling must comply with relevant data protection laws.
   2. Intellectual Property: Users must respect copyright laws and intellectual property rights when creating, sharing, or using digital content.
   3. Appropriate Content: Accessing, creating, or disseminating content that is illegal, offensive, discriminatory, defamatory, pornographic, or otherwise inappropriate is strictly prohibited.
   4. Device Management: All devices connected to the institution's network must comply with the security policies and be regularly updated to prevent security risks.
   5. Social Media and Communication: Users are expected to maintain professionalism and respect when using social media and other communication channels affiliated with The Wheels Project.
   6. Personal Use: The Wheels Project permits the incidental use of the I.T. resources to send personal email, browse the internet and make personal telephone calls, subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. The Wheels Project may withdraw permission for it at any time or restrict access at its discretion. Personal use must meet the following conditions:
      1. it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);
      2. it must not affect your work or interfere with the organisation; and
      3. it must comply with The Wheels Project’s policies, including this policy.
3. **Access and Authorisation**
   1. User Accounts: Individual user accounts will be provided, granting access to specific I.T. resources based on roles and responsibilities. Sharing user accounts is strictly prohibited to maintain accountability and data security. Each user is responsible for the security of the equipment allocated to them. Users must not use personal accounts to send or receive The Wheels Project information.
   2. Password Security: Users must create strong passwords and keep them confidential. Passwords must be changed regularly and never shared with others. A strong password:
      1. is at least 10 characters in length;
      2. does not contain your username; and
      3. contains uppercase and lowercase characters, a number, and a non-alphabetic character (for example, $, \*, !, %).
   3. Device Security: Users must lock their terminals and log off when leaving it unattended, to prevent unauthorised users accessing the system.
   4. Remote Access: Users must ensure that portable devices such as laptops, tablets, and mobile phones used to access the I.T. resources are secured with a strong password to ensure that confidential data is protected in the event of loss or theft.
   5. Restricted Access: Users should never access the following from or via the I.T. resources or using a device issued by The Wheels Project: online radio, audio and video streaming (including streaming of, or downloading of, television radio or films), instant messaging, gaming, or social networking sites (including, but not limited to, Facebook, Twitter, YouTube, Google+, Instagram, Snapchat, Pinterest, Tumblr, Second Life). The Wheels Project may block or restrict access to a website at its discretion.
4. **Systems and Data Security**
   1. System Use: Users must not delete, destroy, or modify existing systems, programs, information, or data (except as authorised).
   2. Third-Party Devices: Users must not attach any device or equipment, such as USB flash drive, MP3 player, tablet, or mobile phone, to The Wheels Project I.T. resources without authorisation from the Office Manager.
   3. Third-Party Networks: Do not connect The Wheels Project devices to a third-party network unless you are connecting to a secure and trusted corporate or home wireless network. Do not connect to public wi-fi networks.
   4. Security Updates: Users must immediately download the latest security patches as notified to them by the IT team/Office Manager.
5. **Email**
   1. Email Risks: Users must exercise particular caution when opening unsolicited emails from unknown sources or emails which appear suspicious.
   2. Professional Communication: Users must adopt a professional tone and observe appropriate etiquette when communicating with third parties by email. Remember that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.
6. **Monitoring**
   1. Monitoring: Our systems enable The Wheels Project to monitor telephone, email, voicemail, internet, and other communications, including any personal use of them (as authorised by The Wheels Project).
   2. Retrieval: We reserve the right to retrieve the contents of email messages or check internet usage as reasonably necessary to fulfil The Wheels Project’s organisational purposes, including but not limited to the following purposes:
      1. to monitor whether use of the I.T resources is legitimate and in accordance with this policy;
      2. to find lost messages or to retrieve messages lost due to computer failure;
      3. to assist in the investigation of alleged wrongdoing; and/or
      4. to comply with any legal obligation.
7. **Reporting Misuse and Violations**
   1. Investigation: Alleged policy violations will be promptly investigated, and appropriate disciplinary action will be taken if necessary.
   2. Reporting: Users must actively participate in safeguarding The Wheels Project’s I.T. infrastructure by immediately reporting any security breaches, suspicious activities, or potential vulnerabilities which they become aware of to the Office Manager.
8. **Training and Awareness**
   1. Education: The Wheels Project will provide regular training and resources to enhance users' awareness of I.T. policies, cybersecurity best practices, and digital literacy.
9. **Enforcement and Consequences**
   1. Compliance: Non-compliance with this policy may result in disciplinary action, ranging from warnings and loss of I.T. privileges to legal consequences in severe cases.
   2. Consistency: Enforcement will be applied consistently, regardless of the individual's position or status within The Wheels Project.
10. **Return of Devices**
    1. Return: If a user has been allocated a device such as a laptop, mobile phone, or tablet, they must be returned to The Wheels Project when the user leaves The Wheels Project.
11. **Updates**
    1. The policy will be reviewed and updated periodically to adapt to changing I.T. landscapes and educational needs.