IT ACCEPTABLE USE POLICY

NATIONAL TRACTION ENGINE TRUST

IT ACCEPTABLE USE POLICY

1. Purpose

The purpose of this IT Acceptable Use Policy is to outline the acceptable use of all IT resources, including computer hardware and software, network systems, internet access, email systems, and other electronic communication systems, by trustees, volunteers, representatives, contractors, and third-party service providers at the National Traction Engine Trust (the "NTET"). This policy aims to protect the integrity, confidentiality, and availability of the NTET's IT resources and to promote responsible and ethical behaviour when using these resources.

2. Scope

This policy applies to all the NTET trustees, representatives, volunteers, contractors, and other individuals who have access to the organisation's IT resources. The NTET seeks to promote the effective and secure use of IT systems to support its mission, ensuring compliance with all relevant laws and regulations.

3. Acceptable and Unacceptable Uses

3.1. Users are encouraged to use the NTET's IT resources to support their responsibilities and advance the organisation's objectives. Personal use is permitted as a privilege, not a right, and must meet the following conditions:

3.1.1. It does not interfere with work duties or organisational operations.
3.1.2. It complies with the NTET's policies and procedures.
3.1.3. It does not place undue demand on IT resources.

3.2. All users of the NTET's IT resources must comply with applicable laws and regulations, including the Data Protection Act 2018, General Data Protection Regulation (GDPR), and NTET's Information Security Policy.

3.3. Users must maintain the security of the NTET's IT resources by using strong passwords, regularly updating software, and reporting suspicious activity to the IT administrator.

3.4. Users must respect the privacy of others and must not access, use, or disclose personal information without authorisation.

3.5. Compliance with all requests from the NTET management regarding IT usage is mandatory.

3.6. NTET IT resources must not be used for:

3.6.1. Downloading, creating, or sharing offensive, obscene, defamatory, or unlawful material.
3.6.2. Activities that facilitate harassment, bullying and/or victimisation.
3.6.3. Activities that promote discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.
3.6.4. Disseminating spam, chain emails, or bulk unsolicited messages.
3.6.5. Activities that infringe intellectual property or privacy rights.
3.6.6. Engaging in fraud, impersonation, or deception.
3.6.7. Introducing malicious software, viruses, or conducting unauthorised penetration testing.

3.7. Misuse of the NTET's networks includes:

3.7.1. Accessing unauthorised information or systems.
3.7.2. Sharing passwords or access credentials.
3.7.3. Disrupting IT systems or other users' work.
3.7.4. Using IT resources for commercial purposes without prior approval.
3.7.5. Installing unauthorised software or hardware.

4. Use of NTET Email and Communication Systems

4.1. NTET's email and messaging systems are for official use. Users must:

4.1.1. Use clear and respectful language.
4.1.2. Avoid sending large attachments or chain messages.
4.1.3. Refrain from sending confidential information without encryption.

4.2. Prohibited uses include:

4.2.1. Harassment or threats.
4.2.2. Promoting personal commercial interests.
4.2.3. Sharing inappropriate or offensive material.

5. Monitoring and Enforcement

5.1. Monitoring the NTET reserves the right to monitor IT usage to ensure compliance with this policy. This includes activity on networks, emails, and internet access.

5.2. Users found in violation of this policy may face:

5.2.1. Restriction or termination of IT access.
5.2.2. Disciplinary action, up to and including dismissal.
5.2.3. Reporting to law enforcement for illegal activities.

6. Exceptions and Exemptions

Requests for exemptions, such as access to sensitive materials for legitimate purposes, must be approved by the NTET's IT administrator or designated authority.

7. Review and Updates

This policy will be reviewed annually or following significant changes in IT infrastructure, regulations, or organisational needs.

For questions or further guidance, please contact:

Email: general.secretary@ntet.co.uk