Review Date- 01/10/2025

Trinity Support Services: Acceptable Use Policy

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to establish clear guidelines for the proper, ethical, and lawful use of technology, including devices, networks, systems, and data at Trinity Support Services (TSS). This policy applies to all employees, contractors, and third-party service providers who have access to the company's IT infrastructure. Its goal is to protect TSS, its clients, and its employees while ensuring that all users understand their responsibilities in maintaining the security and integrity of TSS's digital environment.

2. Scope

This policy applies to all users who access, operate, or manage TSS's technology systems, including but not limited to:

- Company-owned laptops, desktops, mobile devices, and other hardware.
- Email systems, internet access, and intranet resources.
- Cloud services and any remote access technologies.
- Sensitive client data, particularly information related to Edge of Care Services and Return Home Interview Services.

3. Acceptable Use of Company Systems

Employees and contractors are expected to use company resources responsibly. Acceptable uses of TSS technology include:

1. Work-related activities:
    - Accessing, storing, and processing information directly related to work activities at TSS.
    - Communicating with clients, colleagues, and authorised third parties for the purpose of delivering services or maintaining business operations.
2. Compliance with Laws and Policies:
    - All users must comply with relevant UK laws and TSS policies, including data protection regulations (GDPR), confidentiality agreements, and ethical standards.
3. Security Awareness:
    - All employees must maintain the security of their accounts and devices by using strong passwords and regularly updating them. Users are responsible for safeguarding their login credentials.
4. Responsible Use of Internet and Email:
    - The company's internet and email systems must be used for legitimate business purposes. Occasional, limited personal use is allowed if it does not interfere with work responsibilities and adheres to this policy.

4. Prohibited Use

The following activities are strictly prohibited:

1. Unauthorised Access:
    - Accessing or attempting to access any system, account, data, or resource for which the user does not have permission is prohibited. This includes accessing client information without proper authorization or need.
2. Misuse of Sensitive Data:
    - Employees must not copy, disclose, alter, or distribute confidential client information (such as personal data from Edge of Care and Return Home Interview services) unless properly authorised.
    - Transferring client data to unauthorised third parties or personal devices is strictly forbidden.
3. Installation of Unauthorised Software:
    - Users may not install or download any software, applications, or programs on TSS systems without prior approval from TSS's IT department or M&M Information Technologies (M&M IT). This includes file-sharing software, which poses a security risk.
4. Personal Devices:
    - Use of personal devices to conduct TSS business or access company systems without explicit authorization is not allowed. Employees must use company-issued devices when handling sensitive data or accessing company networks.
5. Illegal or Inappropriate Activities:
    - Engaging in activities that violate UK laws, such as uploading, downloading, or distributing illegal or pirated content, is strictly prohibited.
    - Accessing or sharing offensive, discriminatory, or inappropriate content (such as hate speech, pornography, or materials that violate TSS's core values) is also forbidden.
6. Cybersecurity Threats:
    - Any action that introduces a security threat, including spreading malware, viruses, or engaging in activities that could lead to a data breach, will result in disciplinary action.
    - Deliberately bypassing security measures, such as firewalls or encryption, is prohibited.

5. Email and Communication Use

When using TSS's email and communication systems, users must:

1. Professional Conduct:
    - Ensure all communications are respectful, clear, and professional, especially when communicating with clients, partners, or external stakeholders.
2. No Personal Use of Business Email:
    - Employees must refrain from using TSS business email addresses for personal use, such as personal shopping accounts, newsletters, or non-work-related correspondence.
3. Avoid Phishing and Scams:

- Users must remain vigilant for phishing attempts or suspicious emails. Any suspicious activity should be immediately reported to M&M IT or the TSS IT department.

6. Monitoring and Privacy

TSS reserves the right to monitor the use of its technology systems to ensure compliance with this policy. Monitoring may include:

- Internet usage and browsing activities.
- Emails and digital communications sent or received using TSS systems.
- Device logs and activity on company-issued devices.

All users should be aware that their activities on company systems may be subject to review. However, TSS will respect employee privacy as much as possible and will only monitor activities for legitimate business purposes, in compliance with UK privacy laws.

7. Data Security and Storage

Users must follow these guidelines to protect the integrity and confidentiality of TSS data:

1. Secure Storage:
   - All sensitive and confidential data must be stored securely on company-approved systems, such as encrypted drives or cloud services managed by M&M IT. Storing sensitive data on unapproved external devices is prohibited.
2. Backup Procedures:
   - M&M IT will regularly back up company data, but employees are responsible for saving their work on appropriate systems, following TSS's backup guidelines.
3. Data Breaches:
   - In the event of a suspected data breach, users must immediately notify the TSS Data Protection Officer (DPO) and follow the company's incident response procedures.

8. Reporting Violations

Employees who become aware of any violations of this policy must report the issue to their supervisor, TSS IT Department, or the Data Protection Officer. Failure to report misuse may result in disciplinary action.

9. Disciplinary Action

Any violation of this policy may result in disciplinary action, including but not limited to:

- Revocation of access privileges.
- Suspension or termination of employment.
- Legal action if the violation results in the breach of UK laws or company regulations.

Serious breaches that involve unauthorised access, illegal activities, or misuse of client data may lead to criminal prosecution under the Computer Misuse Act 1990, Data Protection Act 2018, and GDPR.

10. Policy Review

This Acceptable Use Policy will be reviewed annually to ensure it remains in line with UK legal requirements and TSS's operational needs.
By adhering to this policy, employees of Trinity Support Services ensure that technology resources are used effectively, securely, and in compliance with all relevant laws and ethical standards.

Contact Information

For questions or concerns regarding this policy, please contact the Company Directors:

Zoe Ashman- zoe.ashman@trinitysupportservices.info

Tracy Dean- Tracy.dean@trinitysupportservices.info