

USING USER SCIENCE. DATA-DRIVEN. THINKING BOLDLY.

TRACKITA PTY LTD: PHONE & INTERNET USE POLICY

Phones and the internet are integral tools for work but can also be sources of distraction or risk if used improperly. This policy establishes guidelines to ensure responsible and lawful use of phones, internet, and related devices at Trackita.

Note:

- 1. This policy does not form part of your employment contract.
- 2. Trackita may amend or withdraw this policy at any time.
- 3. The client's policies for whom you are working are considered Trackita's own policies; where client policies conflict with Trackita's guidelines, the client policies prevail.

1. Phone Usage

1.1 Personal Calls & Messages

- Limited Use: Personal calls or texts must not interfere with work tasks or customer service.
- Emergencies Only: If it's not urgent, please reserve personal calls or texts for breaks or outside working hours.

1.2 Company-Issued Phones

- **Professional Use**: If you receive a company-issued phone, use it primarily for business purposes unless you have specific permission to do otherwise or face an emergency.
- **Reimbursement**: You may be required to reimburse Trackita for personal usage if it exceeds what the company deems reasonable or permissible.

1.3 No Illegal or Offensive Content

- **Zero Tolerance**: Using a company phone for illegal activities, offensive messages, or harassment is strictly forbidden and may result in termination.
- **Client Policy Supremacy**: If you are using a client's phone or network, remember their policies take precedence over Trackita's.

2. Internet & Email Guidelines

2.1 Work-Related Use

- **Primary Purpose**: The internet and email systems should support your job functions.
- **Personal Use**: Seek manager approval for occasional personal browsing or email checks.

2.2 Prohibited Activities

- **Inappropriate Content**: Do not access or distribute materials that are illegal, harassing, or offensive.
- **Confidentiality**: Refrain from posting or sharing proprietary information about Trackita or its clients.
- **Unauthorized Access**: Do not attempt to breach security on any systems—internal or external—without explicit authorization.

2.3 Passwords & Security

- **Disclosure Requirement**: Provide any work-related passwords to management upon request.
- **Return of Assets**: Upon leaving Trackita, return all company equipment and information, including login credentials.
- **Others' Accounts**: Do not use another person's login to circumvent these rules.

3. Consequences of Misuse

- **Disciplinary Action**: Non-compliance with this policy may result in disciplinary measures, up to and including termination of employment.
- Legal Liability: Illegal activities conducted via Trackita equipment or networks may also lead to legal consequences.

4. Related Policies

The client's policies for whom you are working are considered Trackita's own policies; where client policies conflict with Trackita's guidelines, the client policies prevail. Additionally, please review:

Code of Conduct

- Social Media Policy
- Anti-Bullying & Anti-Harassment
- Equal Employment Opportunity and Anti-Discrimination
- Workplace Surveillance Policy

5. Summary

This policy is designed to ensure that Trackita's telecommunication tools—phones, internet, and email—are used responsibly, professionally, and in accordance with both Trackita's standards and the client's policies. Always remember that **the client's policies for whom you are working are considered Trackita's own policies; where there is a conflict, client policies take precedence.** Thank you for exercising responsibility, courtesy, and discretion in your phone and internet use.