

MadeUpName, LLC

Acceptable Use of Technology Policy

Purpose

This policy ensures that all company technology resources are used responsibly, securely, and in a manner that supports MadeUpName, LLC's business objectives. It outlines expectations for using company systems, devices, networks, and data.

Scope

This policy applies to all employees, contractors, and interns who access company-owned or managed technology resources, including laptops, mobile devices, email, cloud systems, and communication tools.

1. Acceptable Use

Company technology resources must be used primarily for business purposes. Limited personal use is acceptable if it does not:

- Interfere with work performance.
- Violate company policies.
- Expose the company to security risks or reputational harm.

2. Prohibited Activities

Users must not:

- Access or distribute offensive, discriminatory, or illegal content.
- Share confidential information with unauthorized parties.
- Install unauthorized software or alter system configurations.
- Use company systems for personal financial gain, political activity, or external business ventures.
- Connect unapproved personal devices to company networks.

3. Security Practices

All users must:

- Use strong passwords and enable multi-factor authentication (MFA).
- Lock devices when unattended.
- Store sensitive data only on company-approved systems.
- Report lost or stolen devices immediately to IT.
- Avoid using public Wi-Fi without a secure VPN connection.

4. Email and Communication Tools

- Company email and messaging platforms (e.g., Slack, Zoom, Google Workspace) must be used professionally and respectfully.
- Phishing or suspicious emails must be reported to IT immediately.
- Users should not represent personal opinions as those of the company.

5. Remote Work Guidelines

Remote employees must maintain secure home networks, update software regularly, and protect company data in accordance with the Remote & Hybrid Work Policy.

6. Data Protection

Users are required to comply with the Data Protection & Privacy Policy when handling company or client data. Unauthorized copying, sharing, or storage of data is prohibited.

7. Monitoring and Privacy

MadeUpName, LLC reserves the right to monitor the use of company systems to ensure compliance with this policy. Monitoring will be conducted lawfully and respectfully, balancing security with privacy.

8. Violations

Any misuse of technology resources may result in disciplinary action, up to and including termination, and possible legal action.

9. Related Policies

This policy should be read alongside the Data Protection & Privacy Policy and AI & Automation Usage Policy.

Effective Date: January 2025

Next Review Date: January 2026

Policy Owner: Human Resources Department