# ACCEPTABLE USE OF TECHNOLOGY POLICY

JANUARY 2026

POLICY NUMBER: TMG-SEC-039
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

## 1. PURPOSE

This Acceptable Use of Technology Policy establishes guidelines for the appropriate use of The Mazi Group's technology resources. Proper use of technology protects company assets, ensures security, and maintains productivity across all brands: Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo.

## 2. SCOPE

This policy applies to:

- All employees, contractors, and temporary workers
- All company-provided technology resources
- Personal devices used for company business (BYOD)
- All brands and business units
- All geographic locations

## 3. TECHNOLOGY RESOURCES COVERED

- Computers, laptops, and tablets
- Mobile phones and smartphones
- Email and messaging systems
- Internet and network access
- Software and applications
- Cloud services and storage
- Printers and peripherals
- Phone systems

## 4. GENERAL PRINCIPLES

- Technology resources are provided for business purposes
- Limited personal use is permitted if it does not interfere with work
- Users are responsible for protecting company resources
- All use must comply with laws and company policies
- The company may monitor use of its resources

# 5. ACCEPTABLE USE

## 5.1 Permitted Activities

- Business-related work and communications
- Professional development and learning
- Limited personal use during breaks
- Accessing approved applications and services

## 5.2 User Responsibilities

- Use technology responsibly and professionally
- Protect login credentials
- Lock devices when unattended
- Report security incidents
- Keep software updated
- Follow data protection requirements

# 6. PROHIBITED ACTIVITIES

## 6.1 Strictly Prohibited

- Accessing, downloading, or distributing illegal content
- Pornography or sexually explicit material
- Harassment, discrimination, or threatening communications
- Unauthorized access to systems or data
- Installing unauthorized software
- Circumventing security controls
- Sharing login credentials
- Using company resources for personal business
- Cryptocurrency mining
- Excessive personal use affecting productivity

## 6.2 Activities Requiring Approval

- Installing non-standard software

- Connecting personal devices to network
- Accessing company data from personal devices
- Using cloud storage services
- Remote access setup

## 7. EMAIL AND MESSAGING

### 7.1 Appropriate Use

- Professional and respectful communications
- Accurate representation of identity
- Appropriate use of company signature
- Proper handling of confidential information

### 7.2 Prohibited

- Sending harassing or offensive messages
- Forwarding chain letters or spam
- Sending confidential information to unauthorized recipients
- Using personal email for company business
- Auto-forwarding company email to personal accounts

### 7.3 Email Security

- Be cautious of phishing attempts
- Do not click suspicious links
- Report suspicious emails to IT
- Encrypt sensitive information

## 8. INTERNET USE

### 8.1 Appropriate Use

- Business-related research and activities
- Professional networking
- Limited personal browsing during breaks

### 8.2 Prohibited

- Accessing inappropriate websites
- Downloading unauthorized content
- Streaming excessive non-work content
- Using anonymizers or proxies to bypass controls
- Engaging in illegal activities

### 8.3 Web Filtering

- Company may filter web access
- Certain categories blocked
- Request exceptions through IT if needed for work

## 9. MOBILE DEVICES

### 9.1 Company-Provided Devices

- Primarily for business use
- Keep device secure
- Use strong passcode/biometric
- Enable remote wipe capability
- Report lost/stolen devices immediately

### 9.2 Personal Devices (BYOD)

- Must be approved by IT
- Must meet security requirements
- Mobile device management (MDM) may be required
- Company data must be protected
- Company may wipe company data remotely

## 10. SOFTWARE AND APPLICATIONS

### 10.1 Approved Software

- Use only approved and licensed software

- Request new software through IT
- Keep software updated

### 10.2 Prohibited

- Installing unauthorized software
- Using pirated or unlicensed software
- Disabling security software
- Using unapproved cloud services for company data

### 10.3 AI Tools

- Use only approved AI tools
- Do not input confidential data into public AI services
- Follow AI ethics policy (TMG-SEC-038)

## 11. DATA PROTECTION

- Protect confidential and personal data
- Store data in approved locations
- Do not store company data on personal devices without approval
- Encrypt sensitive data
- Follow data classification guidelines
- Properly dispose of data when no longer needed

## 12. REMOTE WORK

- Secure home network
- Use VPN for company access
- Protect devices from unauthorized access
- Maintain physical security of devices
- Follow same policies as in office

## 13. SOCIAL MEDIA

- Follow social media policy (TMG-SEC-029)

- Do not share confidential information
- Be thoughtful about company-related posts
- Separate personal and professional accounts

## 14. MONITORING

### 14.1 Company Rights

- Company may monitor use of its technology resources
- No expectation of privacy on company systems
- Monitoring may include email, internet, files
- Monitoring conducted in compliance with law

### 14.2 Purpose of Monitoring

- Security threat detection
- Policy compliance
- Legal and regulatory requirements
- Performance and capacity management

## 15. INCIDENT REPORTING

Report immediately to IT Security:

- Lost or stolen devices
- Suspected security breaches
- Malware or virus infections
- Phishing attempts
- Unauthorized access
- Policy violations

## 16. CONSEQUENCES OF VIOLATIONS

Violations may result in:

- Revocation of technology privileges
- Disciplinary action up to termination

- Legal action
- Personal liability for damages

## 17. TRAINING

- Security awareness training for all employees
- Training on this policy
- Regular refresher training
- Phishing awareness exercises

## 18. ROLES AND RESPONSIBILITIES

### 18.1 Employees

- Comply with this policy
- Protect company resources
- Report incidents
- Complete required training

### 18.2 IT Department

- Implement security controls
- Manage technology resources
- Respond to incidents
- Provide user support

### 18.3 Managers

- Ensure team compliance
- Address violations
- Support security initiatives

## 19. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-016: Data Privacy and Protection Policy

- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-024: Employee Handbook and Workplace Policies
- TMG-SEC-029: Social Media and Influencer Marketing Policy

## 20. POLICY REVIEW

This policy shall be:

- Reviewed annually by IT and HR
- Updated for technology changes
- Approved by CTO and CHRO
- Communicated to all employees

## 21. DEFINITIONS

- **Technology Resources:** All company-provided hardware, software, and services.
- **BYOD:** Bring Your Own Device - personal devices used for work.
- **MDM:** Mobile Device Management - software to manage mobile devices.
- **VPN:** Virtual Private Network - secure connection to company network.

**For questions or to report incidents:**
Technology Department
security@mazigroup.us