# GoZupees Acceptable Use Policy

**Document Version:** 1.0  
**Effective Date:** January 2025  
**Review Date:** January 2026  
**Owner:** IT/HR Team  
**Approved By:** [CEO/CTO]

## Purpose and Scope of Acceptable Use

This Acceptable Use Policy establishes clear guidelines for the appropriate use of GoZupees' technology resources, systems, and services by all employees, contractors, and authorized users. As an artificial intelligence technology company that develops sophisticated AI solutions for enterprise clients, we must maintain the highest standards of professional conduct and system usage to protect our intellectual property, client data, and business reputation while enabling productive and innovative work.

The scope of this policy encompasses all technology resources provided or managed by GoZupees, including but not limited to computer systems, mobile devices, network infrastructure, cloud services, software applications, and data storage systems. This policy applies to all individuals who have been granted access to GoZupees technology resources, regardless of their employment status, location, or the device ownership model under which they access our systems.

Our approach to acceptable use recognizes that technology resources are essential tools for conducting business and that reasonable personal use may occur within appropriate boundaries. However, all use of GoZupees technology resources must be consistent with our business objectives, legal obligations, and ethical standards. Users are expected to exercise good judgment and professional discretion in their use of technology resources and to understand that all activities conducted using our systems may be monitored and logged for security and compliance purposes.

The principles underlying this policy emphasize respect for intellectual property rights, protection of confidential information, compliance with applicable laws and regulations, and maintenance of professional standards that reflect positively on GoZupees and support our mission of delivering innovative AI technologies to our clients. Users who violate this policy may face disciplinary action up to and including termination of employment or access privileges.

This policy is designed to be practical and enforceable while providing sufficient flexibility to accommodate the diverse work requirements of our distributed team and the evolving nature of AI technology development. Regular review and updates ensure that the policy remains relevant and effective as our business and technology environment continues to evolve.

## General Principles and Responsibilities

All users of GoZupees technology resources share fundamental responsibilities for maintaining the security, integrity, and appropriate use of our systems and data. These responsibilities extend beyond mere compliance with technical requirements to encompass ethical behavior, professional judgment, and active participation in protecting our collective technology assets and business interests.

Users must respect the confidentiality and privacy of information stored on or transmitted through GoZupees systems, recognizing that our technology resources often contain sensitive client data, proprietary algorithms, and confidential business information that requires careful protection. This includes understanding and implementing appropriate access controls, handling sensitive information according to established classification guidelines, and reporting potential security incidents or policy violations promptly and accurately.

Professional conduct in the use of technology resources means conducting oneself in a manner that reflects positively on GoZupees and supports our business objectives and client relationships. This includes using technology resources primarily for legitimate business purposes, avoiding activities that could damage our reputation or business relationships, and maintaining appropriate standards of communication and behavior in all technology-mediated interactions.

Legal compliance requires that all use of technology resources comply with applicable laws and regulations, including intellectual property laws, privacy and data protection regulations, employment laws, and industry-specific requirements that may apply to our business operations or client relationships. Users are responsible for understanding the legal implications of their technology use and for seeking guidance when uncertain about the legality or appropriateness of specific activities.

Resource stewardship involves using technology resources efficiently and responsibly, recognizing that these resources represent significant investments that must be protected and maintained for the benefit of the entire organization. This includes avoiding wasteful or excessive use of system resources, protecting equipment from damage or theft, and reporting technical problems or maintenance needs promptly to ensure continued system availability and performance.

Continuous learning and adaptation recognize that technology environments and security threats evolve rapidly, requiring users to stay informed about new policies, procedures, and best practices that affect their use of technology resources. Users are expected to participate in required training programs, stay current with policy updates, and adapt their practices as necessary to maintain compliance with evolving requirements.

## Authorized and Prohibited Uses

Technology resources provided by GoZupees are intended primarily for legitimate business purposes that support our mission of developing and delivering innovative AI solutions to our clients. Authorized uses include all activities that directly support job responsibilities, professional development, and business objectives, as well as reasonable personal use that does not interfere with business operations or violate other provisions of this policy.

Business-related activities that are explicitly authorized include accessing and using business applications and systems necessary for job performance, communicating with clients, colleagues, and business partners through approved channels, conducting research and development activities related to AI technologies and business opportunities, and participating in training and professional development programs that enhance job performance and career growth.

Reasonable personal use of technology resources is permitted when such use does not interfere with business operations, consume excessive system resources, or violate other provisions of this policy. Personal use should be limited in scope and frequency and should not create security risks or legal liabilities for GoZupees. Examples of acceptable personal use include brief personal communications during breaks, accessing news and information websites during personal time, and using business devices for personal activities while traveling for business purposes.

Prohibited uses include any activities that are illegal, unethical, or inconsistent with GoZupees' business objectives and professional standards. Specifically prohibited activities include accessing, downloading, or distributing illegal or inappropriate content such as pornography, hate speech, or copyrighted material without proper authorization, using technology resources for personal business ventures or commercial activities unrelated to GoZupees, and engaging in activities that could compromise system security or violate the privacy rights of others.

Harassment, discrimination, or other inappropriate behavior conducted through technology resources is strictly prohibited and may result in immediate disciplinary action. This includes sending offensive or threatening communications, accessing or sharing inappropriate content, and using technology resources to create hostile or uncomfortable work environments for colleagues or clients.

Activities that compromise system security or integrity are prohibited regardless of intent, including attempting to gain unauthorized access to systems or data, installing unauthorized software or hardware, circumventing security controls or monitoring systems, and engaging in activities that could introduce malware or other security threats to our technology environment.

## Internet and Email Usage Guidelines

Internet access provided by GoZupees is intended to support business activities and professional development while enabling reasonable personal use within appropriate boundaries. Users are expected to exercise professional judgment and discretion in their internet usage and to understand that all internet activities conducted through GoZupees systems may be monitored and logged for security and compliance purposes.

Professional internet usage includes accessing websites and online resources that support job responsibilities, research and development activities, professional learning and development, and legitimate business communications. Users should prioritize business-related internet activities during work hours and should ensure that personal internet use does not interfere with productivity or consume excessive bandwidth or system resources.

Email communications through GoZupees systems must maintain professional standards and comply with applicable laws and regulations regarding business communications, privacy, and data protection. Users are responsible for ensuring that email communications are appropriate for business use, properly secured when containing sensitive information, and compliant with client requirements and regulatory obligations that may apply to specific types of communications.

Security considerations for internet and email usage include being vigilant about phishing attempts and other social engineering attacks, avoiding suspicious websites and downloads that could introduce malware or security threats, using appropriate encryption and security measures for sensitive communications, and reporting potential security incidents or suspicious activities promptly to the IT security team.

Content filtering and monitoring systems are implemented to protect GoZupees systems and users from security threats and inappropriate content. Users should understand that these systems may block access to certain websites or content and should not attempt to circumvent these protections. Requests for access to blocked content for legitimate business purposes should be directed to the IT team for evaluation and potential approval.

International and remote usage considerations apply to users who access internet and email services while traveling or working from international locations. Users should be aware of local laws and regulations that may affect internet usage, understand the additional security risks associated with international internet access, and implement appropriate security measures such as VPN connections when accessing GoZupees systems from foreign locations.

## Software and Application Management

Software installation and management on GoZupees systems must follow established procedures that ensure security, licensing compliance, and system stability while enabling users to access the tools and applications necessary for effective job performance. All software installations must be approved through appropriate channels and must comply with our security standards and licensing requirements.

Approved software includes applications that have been evaluated and authorized by the IT team for business use, open source software that has been reviewed for security and licensing compliance, and personal productivity applications that do not create security risks or licensing violations. Users should request approval for new software installations through established procedures and should not install unauthorized software on business systems.

Software licensing compliance requires that all software used on GoZupees systems be properly licensed and used in accordance with applicable license terms and conditions. Users are responsible for understanding the licensing requirements for software they use and for ensuring that their usage complies with license restrictions regarding the number of installations, permitted uses, and other terms that may apply to specific software products.

Security considerations for software management include ensuring that all software is kept current with security updates and patches, avoiding software from untrusted sources that could introduce malware or security vulnerabilities, and reporting software-related security issues or suspicious behavior promptly to the IT team for investigation and remediation.

Cloud applications and software-as-a-service platforms used for business purposes must be approved and configured in accordance with our security and data protection requirements. Users should not sign up for cloud services using business email addresses or upload business data to unauthorized cloud platforms without proper approval and security review.

Personal software and applications may be installed on business devices in limited circumstances, provided that such installations do not create security risks, violate licensing requirements, or interfere with business operations. Personal software installations should be minimal and should be removed when no longer needed or when requested by the IT team.

## Data Handling and Information Security

Data handling practices must ensure that all information stored on or transmitted through GoZupees systems receives appropriate protection based on its classification and sensitivity level. Users are responsible for understanding the classification of information they work with and for implementing appropriate handling and protection measures that comply with our data protection policies and applicable legal requirements.

Confidential and proprietary information, including client data, AI algorithms, business strategies, and other sensitive information, must be handled with special care to prevent unauthorized access, disclosure, or misuse. This includes storing confidential information in approved locations with appropriate access controls, transmitting sensitive information using approved encryption methods, and limiting access to confidential information to individuals who have a legitimate business need to know.

Personal data and privacy protection require special attention to ensure compliance with applicable privacy laws and regulations, including GDPR, UK Data Protection Act, and other privacy requirements that may apply to our business operations or client relationships. Users must understand their responsibilities for protecting personal data and must implement appropriate technical and organizational measures to ensure that personal data is processed lawfully and securely.

Data backup and recovery responsibilities include ensuring that important business data is properly backed up according to established schedules and procedures, understanding how to access backup data when needed for business continuity purposes, and reporting data loss or corruption incidents promptly to enable effective recovery and minimize business impact.

Data retention and disposal practices must comply with established policies and legal requirements regarding how long different types of information should be retained and how it should be securely disposed of when no longer needed. Users should understand the retention requirements for information they work with and should follow established procedures for secure data disposal when information reaches the end of its retention period.

Cross-border data transfer considerations apply when information is transmitted or stored in different countries or jurisdictions, particularly when personal data is involved. Users should understand the legal requirements for international data transfers and should implement appropriate safeguards to ensure that such transfers comply with applicable privacy laws and contractual obligations.

## Mobile Device and Remote Access

Mobile devices used for business purposes, whether company-owned or personally-owned devices used under bring-your-own-device policies, must be configured and managed in accordance with our security standards to protect business information and maintain appropriate access controls. Users are responsible for implementing required security measures and for reporting lost or stolen devices promptly to enable appropriate response measures.

Device security requirements include enabling strong authentication methods such as PINs, passwords, or biometric authentication, installing and maintaining current security software and operating system updates, encrypting device storage to protect information in case of device loss or theft, and enabling remote wipe capabilities that allow business data to be removed if devices are compromised or lost.

Remote access to GoZupees systems and data must be conducted through approved methods and must comply with our security requirements for remote connectivity. This includes using approved VPN connections when accessing business systems from remote locations, implementing appropriate security measures for home networks and internet connections, and understanding the additional security risks associated with remote access from various locations.

Application and data management on mobile devices requires careful attention to ensure that business applications and data are properly secured and that personal and business information are appropriately separated. Users should install only approved business applications, avoid storing sensitive business information on personal applications or cloud services, and understand how to properly manage and secure business data on mobile devices.

Network security considerations for mobile devices include understanding the risks associated with connecting to public Wi-Fi networks and other unsecured connections, implementing appropriate security measures when using mobile devices on public networks, and avoiding activities that could expose business information to unauthorized access through insecure network connections.

Lost or stolen device procedures require immediate reporting to the IT security team to enable appropriate response measures such as remote data wiping, password changes, and access revocation. Users should understand their responsibilities for reporting device security incidents and should cooperate with incident response procedures to minimize the impact of device compromise.

## Social Media and External Communications

Social media usage by GoZupees employees and contractors can have significant implications for our business reputation and client relationships, requiring careful attention to professional standards and appropriate boundaries between personal and business communications. While we respect individuals' rights to engage in personal social media activities, users must understand how their online activities can affect GoZupees and must conduct themselves appropriately in all online communications.

Professional social media usage that represents or references GoZupees must comply with our communication standards and must be coordinated with appropriate marketing and communications personnel to ensure consistency with our brand and messaging strategies. Employees who are authorized to represent GoZupees on social media platforms must follow established guidelines for professional communications and must ensure that their posts and interactions reflect positively on our company and values.

Personal social media activities should be clearly distinguished from professional activities, and users should avoid creating confusion about whether they are speaking on behalf of GoZupees or expressing personal opinions. When discussing work-related topics on personal social media accounts, users should include appropriate disclaimers and should avoid sharing confidential information or making statements that could damage business relationships or competitive positions.

Confidentiality and intellectual property protection require that users avoid sharing proprietary information, client data, or other confidential business information through social media platforms or other external communications channels. This includes being careful about sharing information about projects, clients, business strategies, or technical developments that could provide competitive advantages to others or violate confidentiality obligations.

Client and business relationship considerations require that users be mindful of how their social media activities might affect client relationships or business partnerships. Users should avoid making negative comments about clients, competitors, or business partners and should understand that their online activities can be viewed by clients and other business contacts who may form opinions about GoZupees based on employee behavior.

Crisis communication and incident response procedures apply when social media activities create potential reputation or business risks for GoZupees. Users should report social media incidents or concerns promptly to appropriate management personnel and should cooperate with any necessary response measures to address potential business impacts.

## Monitoring and Compliance

Technology resource monitoring is conducted to ensure compliance with this policy, protect system security and integrity, and support business operations and legal requirements. Users should understand that their use of GoZupees technology resources may be monitored and logged, and that this monitoring information may be reviewed for security, compliance, and business purposes.

Monitoring activities include network traffic analysis to detect security threats and policy violations, email and communication monitoring to ensure compliance with business and legal requirements, system access logging to track user activities and detect unauthorized access attempts, and performance monitoring to ensure that technology resources are used efficiently and effectively.

Privacy considerations in monitoring activities balance the need for security and compliance oversight with respect for user privacy and personal information. Monitoring activities are conducted in accordance with applicable privacy laws and regulations and are limited to what is necessary for legitimate business purposes. Users are notified about monitoring activities through this policy and other appropriate communications.

Compliance reporting and investigation procedures ensure that policy violations and security incidents are properly documented and addressed. Users who become aware of potential policy violations or security incidents should report them promptly through established channels, and all users are expected to cooperate with compliance investigations and corrective actions as necessary.

Audit and assessment activities may be conducted periodically to evaluate compliance with this policy and to identify opportunities for improvement in our technology resource management and security practices. Users should cooperate with audit activities and should provide accurate information and documentation as requested to support compliance assessment and improvement efforts.

Corrective actions for policy violations may include additional training, changes to access privileges, disciplinary measures, or other actions deemed appropriate based on the nature and severity of the violation. Users should understand that repeated or serious policy violations may result in termination of employment or access privileges and may have legal consequences depending on the nature of the violation.

## Enforcement and Disciplinary Actions

Policy enforcement is conducted fairly and consistently to ensure that all users understand their responsibilities and that violations are addressed appropriately based on their nature and severity. The goal of enforcement activities is to maintain compliance with policy requirements while providing opportunities for education and improvement when violations occur due to misunderstanding or lack of awareness.

Progressive disciplinary measures may be applied for policy violations, beginning with education and counseling for minor or first-time violations and escalating to more serious consequences for repeated or severe violations. The specific disciplinary measures applied will depend on factors such as the nature and severity of the violation, the user's history of compliance, and the potential business impact of the violation.

Immediate suspension or termination of access privileges may be necessary for violations that create significant security risks or legal liabilities, regardless of whether the violation was intentional. Users should understand that certain types of violations, such as unauthorized access to confidential information or installation of malicious software, may result in immediate loss of access privileges pending investigation and resolution.

Legal consequences may apply for violations that involve illegal activities or that create legal liabilities for GoZupees. Users should understand that policy violations may be reported to law enforcement authorities when appropriate and that they may be personally liable for legal consequences resulting from their misuse of technology resources.

Appeal and review procedures are available for users who believe that disciplinary actions have been applied inappropriately or who wish to contest the findings of compliance investigations. Users have the right to request review of disciplinary decisions through established human resources procedures and to present additional information or evidence that may be relevant to their cases.

Documentation and record keeping for enforcement activities ensure that policy violations and disciplinary actions are properly documented for legal and compliance purposes. This documentation may be used in future disciplinary decisions and may be provided to law enforcement authorities or other external parties when required by legal obligations or business necessities.

**Document Control:**

* **Next Review Date:** January 2026
* **Document Owner:** IT/HR Team
* **Approval Authority:** CEO/CTO
* **Distribution:** All personnel with access to GoZupees technology resources

For questions about acceptable use policies, contact: [it-policy@gozupees.com](mailto:it-policy@gozupees.com)