Acceptable Use Policy

This Acceptable Use Policy (this **"Policy"**) describes prohibited uses of the Services provided by GPTW. In accordance with the Agreement, Customer agrees to use the Services in accordance with the latest version of this Policy. Capitalized terms used but not defined in this Policy have the meanings given to them in the Agreement between Customer and GPTW.

1. Prohibited Use.

Customer agrees that it shall not use the Services, nor authorize, encourage, promote, facilitate or instruct others including its authorized users or Affiliates to use the Services as set forth below:

Prohibited use	Descriptions and Examples
(a) No Illegal, Harmful, or Offensive Use or Content	Customer may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include, but are not limited to: • **Illegal Activities.** Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography. • **Harmful or Fraudulent Activities.** Activities that may be harmful to others, GPTW's operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices. • **Infringing Content.** Content that infringes or misappropriates the intellectual property or proprietary rights of others. • **Offensive Content.** Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts. • **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.
(b) No Security Violations	Customer may not use the Services to violate the security or integrity of the Services or any other SaaS or software application, technology network, computer or communications system, data interfaces (*e.g.,* APIs & webhooks), tenant environments, network or computing device, or related infrastructure (each, a "System"). Prohibited activities include, but are not limited to: • **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System. Customer will not perform any security integrity review, penetration test, load test, denial of service simulation or vulnerability scan on any System. • **Interception.** Monitoring of data or traffic on a System without permission. • **Falsification of Origin.** Forging, altering, or removing TCP-IP packet headers, e-mail headers, or any part of a message describing its origin

© 2026 Great Place To Work Institute, Inc. All rights reserved

	or route. This prohibition does not include the use of aliases or anonymous remailers. • **No Use of Robots.** Customer will not use any tool designed to automatically emulate the actions of a human user (e.g., robots).
(c) No Network Abuse	Customer may not make connections to any users, hosts, or Systems unless Customer has permission to communicate with them. Prohibited activities include, but are not limited to: • **Monitoring or Crawling.** Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled. • **Denial of Service (DoS).** Inundating a System or Services with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective. • **Interference.** Interfering with, disrupting, degrading, impairing, or creating any unusual, excessive, or disproportionate burden on the proper functioning, performance, stability, operation, or availability of any System, including any attempt to overload, query, scrape, synchronize, extract, test, benchmark, or otherwise excessively consume system resources beyond ordinary and intended use. Prohibited activities include, but are not limited to, mail bombing, news bombing, broadcast attacks, flooding techniques, excessive automated requests, bulk data extraction, or other activities that, in GPTW's reasonable discretion, materially increase resource consumption, require additional infrastructure, bandwidth, storage, compute capacity, monitoring, support, maintenance, or administrative resources, or negatively affect other customers, users, Systems, or Services. • **Operation of Certain Network Services.** Operating network services, open data stores, or gateways like open proxies, open mail relays, or open recursive domain name servers to access Systems or Services. • **Avoiding System Restrictions.** Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions. • **Excessive Resource Consumption or Non-Ordinary Use.** Using the Services or Systems in a manner that exceeds ordinary, reasonable, or intended usage patterns, or that, in GPTW's reasonable discretion, causes or is likely to cause excessive consumption of processing capacity, memory, storage, bandwidth, input/output operations, support resources, administrative overhead, or other technical or operational resources. Prohibited activities include high-volume extraction or replication of data, excessive synchronization or polling activities, automated or programmatic access that generates disproportionate system load, repeated or unnecessary data interface calls, large-scale reporting or export activities, or any activity that requires GPTW to allocate additional resources, implement mitigation measures, increase service capacity, or otherwise incur additional operational burden to support Customer's use. GPTW may throttle, suspend, condition, limit, or require Customer to modify such activities, migrate to alternative service offerings, or pay additional fees associated with such usage.

© 2026 Great Place To Work Institute, Inc. All rights reserved

(d) No E-Mail or Other Message Abuse	Customer will not use the Services to distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements. Customer will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. Customer will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

2. Monitoring and Enforcement.

GPTW reserves the right, but does not assume the obligation, to investigate any violation of this Policy or misuse of the Services. GPTW may remove, disable access to, or modify any content or resource that violates this Policy.

If Customer violates the Policy or authorizes or helps others to do so, GPTW may suspend use of the Services until the violation is corrected or terminate the Agreement for cause in accordance with the terms of the Agreement. GPTW may modify this Policy at any time by posting a revised version to this URL.

GPTW may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. GPTW's reporting may include disclosing appropriate Customer information. GPTW may also cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

3. Reporting of Violations of this Policy by Customer.

If Customer becomes aware of any violation of this Policy, Customer will immediately notify GPTW and provide GPTW with assistance, as requested, to investigate, stop, and remedy the violation.

© 2026 Great Place To Work Institute, Inc. All rights reserved