terryberry
Engage · Reward · Succeed

ACCEPTABLE USE POLICY (AUP)

This Acceptable Use Policy (this **"AUP"**) describes permitted and prohibited uses of the Terryberry Services. This AUP is incorporated into and forms part of the agreement(s) governing access to and use of the Services between Terryberry and the customer or other contracting entity (the **"Agreement"**). Capitalized terms not defined in this AUP have the meanings given in the Agreement.

1. Scope.

1.1. Scope Generally. This AUP applies to all access to and use of:

a. Terryberry's employee recognition and engagement platforms;

b. milestone and service award programs (including automated anniversary, birthday, and retirement programs);

c. employee listening and survey tools;

d. wellness programs and applications (including step challenges and wellbeing tracking features);

e. incentive programs (including points-based and goal-based programs);

f. any related websites, mobile applications, APIs, software, integrations, support services, fulfillment services, and documentation (collectively, the **"Services"**).

1.2. This AUP applies to the Customer, its Affiliates (if permitted under the Agreement), and all end users, including Customer's employees, contractors, administrators, and other authorized users (collectively, **"Users"**).

2. Acceptable Use; General Principles.

2.1. Permitted Uses. Users may use the Services only:

a. for Customer's internal business purposes in connection with employee recognition, engagement, wellness, survey/listening, and incentive programs (as applicable);

b. in accordance with the Agreement, this AUP, and all applicable laws and regulations;

c. in a manner that is respectful, professional, and consistent with a workplace environment.

2.2. Eligibility; No Consumer Use.

a. Workplace use only. The Services are intended for use in connection with workplace recognition, engagement, wellness, survey/listening, and incentive programs and are not intended for personal, consumer, or household use.

b. Minimum age. Users must be at least eighteen (18) years old (or the minimum age of digital consent in the applicable jurisdiction, if higher) to access or use the Services. Customer is responsible for ensuring that it does not authorize access for individuals who do not meet this requirement.

2.3. General Prohibited SaaS Uses. In addition to the service-specific restrictions in this AUP, Users will not, and will not permit any third party to, do any of the following with respect to the Services:

a. Unauthorized access. Access or attempt to access the Services, systems, data, accounts, workspaces, tenants, or networks other than those expressly authorized; or bypass or defeat access restrictions, authentication measures, or security controls.

b. Interference and abuse of resources. Interfere with, disrupt, or degrade the Services or any other customer's use of the Services; or use the Services in a way that results in excessive, abusive, or anomalous traffic, storage, CPU usage, or bandwidth consumption, including through automated scripts, loops, or non-human traffic.

c. Malicious code and security threats. Introduce malware or harmful code; use the Services to conduct, promote, or distribute phishing, spam, or other abusive communications; or use the

Services to facilitate unauthorized intrusion, exploitation, or security testing without Terryberry's prior written approval.

d. **Circumvention and evasion.** Circumvent any usage limits, technical restrictions, licensing limits, feature gating, or administrative controls; or create or use multiple accounts to avoid restrictions.

e. **Resale and unauthorized commercial use.** Sell, resell, rent, lease, sublicense, timeshare, or otherwise make the Services available to any third party as a service bureau or managed service, except as expressly permitted under the Agreement.

f. **Copying and competitive use.** Reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or underlying ideas, algorithms, or structure of the Services (except to the extent prohibited by applicable law); or use the Services to develop, train, improve, or provide a competing product or service.

g. **Scraping and bulk extraction.** Use robots, spiders, scrapers, or other automated means to access the Services or extract data, except as expressly permitted via the Services' documented APIs and within stated limits.

h. **Infringement.** Post, upload, or share content that infringes third-party intellectual property rights or other proprietary rights.

i. **High-risk use.** Use the Services in any manner where failure of the Services could reasonably be expected to result in death, personal injury, or physical property damage (for example, emergency response, critical medical care, or nuclear facilities), except to the extent expressly agreed in writing.

2.4. **Prohibited Content and Conduct.** Users will not, and will not permit any third party to, use the Services to:

a. **Harassment, Harm, and Inappropriate Content.**

i. post, transmit, store, or share content that is unlawful, threatening, abusive, harassing, defamatory, hateful, discriminatory, obscene, pornographic, or otherwise objectionable;

ii. promote violence or self-harm, or target individuals or groups based on protected characteristics;

iii. engage in bullying, intimidation, doxxing, or stalking;

iv. share content that violates Customer's workplace policies or codes of conduct (including anti-harassment and non-discrimination policies) as applicable.

b. **Fraud, Deception, and Manipulation.**

i. impersonate any person or entity, or misrepresent affiliation with any person or entity;

ii. manipulate program outcomes (including recognition, surveys, leaderboards, challenges, eligibility, or point awards) through deception, collusion, or other improper means;

iii. submit false or misleading survey responses or wellness activity data, including via automation, device spoofing, coordinated falsification, or non-human traffic;

iv. use the Services to promote scams, phishing, or other fraudulent activity.

c. **Privacy and Confidentiality Violations.**

i. post or disclose another person's personal data without appropriate authorization;

ii. post or disclose special category/sensitive data (e.g., health information, biometric identifiers, precise geolocation, government IDs, financial account numbers, or information about minors) unless explicitly supported by the Services and authorized under the Agreement and applicable law;

iii. use the Services to collect, store, or process protected health information regulated by HIPAA, or credit card data subject to PCI DSS, unless the Agreement expressly allows it and the parties have executed any required addenda (e.g., a Business Associate Agreement)

and implemented required controls;

iv. attempt to re-identify or deanonymize survey results or analytics intended to be anonymous or aggregated, including by combining outputs with other datasets.

d. Illegal or Regulated Uses.

i. use the Services in violation of any law or regulation, including employment, labor, privacy, consumer protection, export control, sanctions, anti-bribery, and anti-corruption laws;

ii. use the Services for unlawful employment decisions, including discriminatory hiring, promotion, termination, or compensation practices;

iii. use the Services to monitor or surveil individuals in ways that violate applicable law or Customer's obligations to its workforce (including notice/consent requirements where applicable).

3. Account Access and Credentials.

3.1. Accounts. Users will not:

a. share passwords or authentication credentials, or allow any other person to access the Services using a User's credentials (except where the Services expressly permit delegated access through administrative roles);

b. use shared, generic, or group accounts unless expressly permitted by Terryberry in writing;

c. attempt to access any other customer's data, workspaces, or tenant environments;

d. fail to promptly notify Customer and Terryberry if the User suspects credentials have been compromised or if there is unauthorized access.

3.2. Credentialing. Customer is responsible for administering accounts, roles, and permissions, including promptly disabling credentials for Users who no longer require access.

4. Data Extraction, Directory Harvesting, and Competitive Use.

4.1. Prohibited Uses. Users will not, and will not permit any third party to:

a. harvest, collect, or compile User or employee directories, profile information, email addresses, or other contact information from the Services for any purpose that is not authorized under the Agreement;

b. use the Services or any information obtained through the Services to develop, train, improve, or provide a competing product or service, or to benchmark or competitive-test the Services for the benefit of a third party or a competing product, except as expressly permitted under the Agreement;

c. export, extract, or download data in a manner that is excessive, abusive, or inconsistent with normal use, including by using automated means outside authorized APIs.

5. Program Integrity: Points, Rewards, Awards, and Incentives.

5.1. Restrictions. To protect program integrity and fairness, Users will not:

a. attempt to earn, transfer, trade, or redeem points or rewards through unauthorized means;

b. purchase, sell, barter, or exchange points, rewards, awards, or redemption codes outside the Services (except as expressly permitted by the applicable program rules);

c. create fake accounts, duplicate accounts, or use bots/automation to generate recognition events, challenge activity, survey responses, or other interactions;

d. use recognition, incentive, or wellness programs as gambling or lottery systems, or in a manner that violates applicable sweepstakes, contest, or prize laws;

e. use the Services to facilitate kickbacks, bribery, or improper inducements, including using awards to influence a business decision unlawfully.

5.2. Program Rules. Terryberry may require additional program rules, eligibility criteria, verification steps,

fraud checks, and redemption controls for points, rewards, awards, and redemptions. Program-specific rules, eligibility requirements, and redemption conditions (collectively, **"Program Rules"**) may be presented in the Services, in Documentation, or in ordering materials and are incorporated into this AUP by reference.

6. Physical Awards and Fulfillment.

6.1. Customization. Where the Services support ordering, customizing, or shipping physical awards (e.g., rings, lapel pins, watches, plaques, trophies, and similar items):

- **a.** Users must provide accurate customization content (including names and inscriptions) and accurate shipping and recipient information;
- **b.** Users must not submit customization content that violates Section 5, infringes third-party rights, or would require Terryberry to manufacture or distribute illegal or prohibited items;
- **c.** Users must not redirect shipments, submit fraudulent addresses, or attempt chargeback abuse or other abuse of the ordering process;
- **d.** Users must comply with any applicable export/import laws and sanctions restrictions for shipments.

6.2. Additional Terms. Additional fulfillment, returns, and shipping terms may apply under the Agreement and Program Rules.

7. Wellness Programs; Use Limitations.

7.1. Wellness. Where the Services provide wellness features (including activity tracking, challenges, workshops, and wellbeing metrics):

- **a.** the Services are not medical devices and do not provide medical diagnosis or treatment;
- **b.** Users must not use the Services for emergency purposes or rely on the Services for medical decision-making;
- **c.** Users must not upload medical records, physician notes, insurance information, or other clinical documentation unless expressly supported and authorized in writing by Terryberry;
- **d.** Users must not falsify activity, steps, sleep, mood, nutrition, or other wellbeing metrics (including through device spoofing or automation).

7.2. Customer Responsibility. Customer is responsible for ensuring its wellness program design (including participation requirements, incentives, and communications) complies with applicable employment, privacy, and benefits laws.

8. Employee Listening and Survey Tools; Fair Use and Anti-Retaliation.

8.1. Prohibited Uses. Where the Services provide survey tools, eNPS, sentiment tracking, or retention risk analytics:

- **a.** Users must not attempt to identify an individual respondent where surveys are configured as anonymous or intended to be anonymous or aggregated;
- **b.** Users must not configure, launch, or analyze surveys in a manner designed to infer identity through small cohort targeting, repeated micro-surveys, or combination with other datasets;
- **c.** Customer must not use the Services to retaliate against individuals for survey participation or feedback;
- **d.** Customer must comply with applicable notice and consent obligations and workplace laws regarding monitoring, analytics, and automated decision-making (as applicable).

9. Communications, Messaging, and Community Features.

9.1. Use Restrictions. Where the Services enable social features (e.g., recognition posts, comments, reactions, announcements, and messaging):

- **a.** Users must maintain professional, workplace-appropriate communications;
- **b.** Users must not spam, send bulk unsolicited messages, or use the Services primarily for advertising

or solicitation;

c. Users must not post third-party content that infringes intellectual property rights (copyright, trademark, or trade secret).

d. Users must not submit false, misleading, or bad-faith reports or flags through any reporting, abuse, or moderation features.

10. Confidential Information in Social and Broad-Visibility Areas.

10.1. Users should not post, share, or otherwise make available through recognition feeds, comments, public profiles, announcements, or other broad-visibility areas of the Services any of Customer's or any third party's trade secrets, source code, non-public financial information, security details, or other highly sensitive confidential information, except to the extent the relevant visibility settings limit access to authorized recipients and Customer has authorized such disclosure.

11. User Content; Intellectual Property; DMCA Notices

11.1. User Content License. As between Terryberry and Customer, Customer (or its licensors) retains ownership of content Customer or Users submit to the Services (including recognition posts, comments, images, survey questions, survey responses, and program content) (**"User Content"**), subject to the rights and licenses granted in the Agreement. Customer grants Terryberry and its subcontractors a worldwide, non-exclusive, royalty-free license to host, copy, transmit, display, perform, process, and otherwise use User Content solely as necessary to provide, secure, maintain, and improve the Services, to prevent or address fraud, security, or technical issues, and to comply with law and enforce this AUP and the Agreement.

11.2. DMCA Takedown Notices (U.S. Only). If you believe content available through the Services infringes your copyright, you may submit a notice under the Digital Millennium Copyright Act (the **"DMCA"**) to Terryberry's designated agent: privacy@terryberry.com.

a. A DMCA notice must include:

i. the physical or electronic signature of the copyright owner or a person authorized to act on the owner's behalf;

ii. identification of the copyrighted work claimed to have been infringed (or, if multiple works are covered by a single notice, a representative list);

iii. identification of the material claimed to be infringing and information reasonably sufficient to permit Terryberry to locate the material;

iv. your contact information (address, telephone number, and, if available, email address);

v. a statement that you have a good-faith belief that use of the material is not authorized by the copyright owner, its agent, or the law; and

vi. a statement, made under penalty of perjury, that the information in the notice is accurate and that you are the copyright owner or authorized to act on the owner's behalf.

11.3. Counter-Notification. If you believe your content was removed or disabled in error, you may submit a counter-notification to Terryberry's designated agent at the address above. A counter-notification must include:

a. your physical or electronic signature;

b. identification of the material that has been removed or disabled and the location where the material appeared before it was removed or disabled;

c. a statement under penalty of perjury that you have a good-faith belief the material was removed or disabled as a result of mistake or misidentification; and

d. your name, address, and telephone number, and a statement that you consent to the jurisdiction of the federal district court for the judicial district in which your address is located (or, if outside the U.S., for any judicial district in which Terryberry may be found), and that you will accept service of process from the person who provided the DMCA notice (or an agent of that person).

11.4. Repeat Infringer Policy. Terryberry has a policy to, in appropriate circumstances, suspend or terminate

accounts of Users who are repeat infringers of intellectual property rights.

12. AI / Machine Learning Restrictions.

12.1. Prohibited Uses. Users will not, and will not permit any third party to:

a. use the Services, Documentation, or any data or outputs accessed through the Services (including recognition content, analytics, survey results, and reports) to develop, train, fine-tune, improve, validate, or benchmark any artificial intelligence or machine learning model, including any generative AI model, except as expressly permitted in the Agreement;

b. use automated tools (including AI agents) to access or use the Services in a manner that violates this AUP, exceeds normal human usage patterns, or circumvents technical restrictions.

12.2. This Section 15 does not restrict Terryberry's use of data as permitted under the Agreement, including to provide, secure, maintain, and improve the Services.

13. Integrations, APIs, and Third-Party Systems.

13.1. Customer Obligations. If Customer uses integrations (e.g., HRIS, SSO, collaboration tools, analytics, or device integrations) or APIs:

a. Customer is responsible for ensuring it has the legal right to connect and transfer data between systems and to authorize Terryberry to process such data as described in the Agreement;

b. Users must comply with all applicable third-party terms and policies;

c. Users must not use integrations or APIs to exfiltrate data, bypass controls, or perform prohibited activities.

14. Administrators and Workplace Governance.

14.1. Customer Responsibilities. Customer is responsible for:

a. ensuring Users are authorized, trained, and informed of appropriate use and Customer's internal policies;

b. configuring privacy and administrative settings consistent with applicable law and Customer's policies (including policies applicable to survey anonymity, recognition visibility, and wellness participation);

c. promptly disabling access for Users who no longer require access, and maintaining secure access controls (including SSO and MFA where available);

d. ensuring required notices and consents are provided for workplace data collection and processing, including for wellness programs and employee listening tools;

e. using surveys, analytics, and engagement insights responsibly, including avoiding attempts to identify individuals where results are intended to be anonymous.

15. Security Incident Reporting and Cooperation.

15.1. Report. Customer will promptly notify Terryberry if Customer becomes aware of any actual or suspected unauthorized access to the Services, compromise of any User credentials, or vulnerability that could impact the Services.

15.2. Cooperation. Customer and Users will reasonably cooperate with Terryberry's investigation and remediation efforts, including by providing information reasonably requested by Terryberry and by preserving relevant evidence.

15.3. No public disclosure. Customer and Users will not publicly disclose the existence or details of any vulnerability or security incident affecting the Services without Terryberry's prior written consent, except to the extent required by law.

16. Monitoring; Enforcement; Suspension.

16.1. Investigation and Enforcement. Terryberry has the right, but not the obligation, to investigate suspected violations of this AUP and may take action consistent with the Agreement, including:

a. removing, disabling access to, or restricting content that violates this AUP;

b. suspending or terminating a User's account;

c. suspending or terminating Customer's access to affected Services, in whole or in part, if necessary to protect the Services, Terryberry, Customer, Users, or third parties, to comply with law, or to prevent or address fraud, security, or technical harm;

d. reporting unlawful activity to appropriate authorities where required or appropriate.

16.2. Material Breach. A violation of this AUP constitutes a material breach of the Agreement.

16.3. Terryberry Rights. To the extent permitted by law and the Agreement, Terryberry is not obligated to monitor content or activity, but may do so to maintain Service integrity, address security or operational issues, comply with law, or enforce this AUP.

16.4. Notice. Where reasonably practicable, and except for violations involving security incidents, suspected fraud, unlawful conduct, or imminent risk of harm, Terryberry may provide Customer notice and a reasonable opportunity to cure violations.

17. Reporting Misuse. Customer and Users should report suspected security issues, policy violations, or abusive content through the applicable in-product reporting features. If the report involves threats of violence, self-harm, or imminent harm, Customer should also follow its internal escalation procedures and contact appropriate emergency services.

18. Updates to This AUP. Terryberry may update this AUP from time to time. Unless otherwise stated in the Agreement, updated versions will be effective upon posting or upon reasonable notice to Customer. Continued use of the Services after the effective date constitutes acceptance of the updated AUP.

19. Order of Precedence. If there is a conflict between this AUP and the Agreement, the Agreement controls unless the Agreement expressly states that this AUP controls for the relevant subject matter.