

DOCUMENT RETENTION AND DESTRUCTION POLICY

TrekFreely

A Colorado Nonprofit Corporation

Adopted by the Board of Directors on 6/21/2026

1. PURPOSE

This Document Retention and Destruction Policy (the “Policy”) provides guidelines for the retention and destruction of records held by TrekFreely (the “Corporation”). The Policy is intended to:

1. Ensure that records are retained for legally required periods and for periods useful to the operation of the Corporation;
 2. Ensure the secure and timely destruction of records that are no longer required, consistent with the Corporation’s privacy-first architecture;
 3. Support compliance with applicable federal and state law, including laws governing nonprofit corporations, tax-exempt organizations, privacy, and data protection;
 4. Align record management practices with the Corporation’s published Privacy Policy and related legal notices.
-

2. ADMINISTRATION

2.1 Policy Administrator. The Secretary of the Corporation shall serve as the Policy Administrator and shall be responsible for the implementation, enforcement, and periodic review of this Policy. The Administrator may delegate specific duties to other officers, employees, or contractors.

2.2 Annual Review. The Policy Administrator shall review this Policy at least annually and recommend updates to the Board as needed.

2.3 Training. Directors, officers, employees, volunteers, and contractors with access to Corporation records shall be informed of this Policy.

3. SCOPE

This Policy applies to all records of the Corporation, regardless of format, including paper, electronic, audio, video, and any other medium. Records include, but are not limited to, correspondence, memoranda, contracts, agreements, financial records, meeting minutes, personnel files, electronic communications, and user service data.

4. RETENTION SCHEDULE — CORPORATE AND ADMINISTRATIVE RECORDS

Record Type	Retention Period
Articles of Incorporation and amendments	Permanent
Bylaws and amendments	Permanent
IRS determination letter and Form 1023 / 1023-EZ filings	Permanent
Board and committee meeting minutes	Permanent
Board resolutions and written consents	Permanent
Corporate seal and stock records (if any)	Permanent
Periodic Reports filed with the Colorado Secretary of State	Permanent
Licenses, permits, and registrations	Permanent plus 7 years after expiration
Conflict of Interest disclosures and annual statements	7 years
Policies and procedures (current and superseded)	Permanent

5. RETENTION SCHEDULE — FINANCIAL AND TAX RECORDS

Record Type	Retention Period
Annual audited or reviewed financial statements	Permanent

Record Type	Retention Period
Federal tax returns (Form 990 series)	Permanent
State tax returns and filings	Permanent
General ledger and journal entries	Permanent
Bank statements and reconciliations	7 years
Canceled checks and deposit records	7 years
Invoices, receipts, and supporting documents	7 years
Accounts payable and receivable records	7 years
Expense reports and reimbursement documentation	7 years
Payroll records (if applicable)	7 years
Tax exemption documentation (federal and state)	Permanent
Charitable solicitation registrations	Permanent
Donor records and acknowledgment letters	7 years
Grant agreements and related correspondence	7 years after grant closeout

6. RETENTION SCHEDULE — LEGAL AND CONTRACTUAL RECORDS

Record Type	Retention Period
Contracts and agreements (fully executed)	Permanent
Contracts under negotiation	Until executed or abandoned
Legal correspondence and opinions	Permanent
Litigation files	Permanent
Insurance policies (current and historical)	Permanent
Insurance claims	7 years after resolution

Record Type	Retention Period
Intellectual property records (trademarks, copyrights)	Permanent
Law Enforcement and Data Request records	7 years

7. RETENTION SCHEDULE — HUMAN RESOURCES RECORDS

Record Type	Retention Period
Director and officer roster and appointment records	Permanent
Board Member Commitment Letters and Consents to Serve	Permanent
Employee personnel files (if applicable)	7 years after termination
Volunteer records	3 years after last service
I-9 forms (if applicable)	3 years after hire or 1 year after termination, whichever is later
Benefits records (if applicable)	7 years

8. RETENTION SCHEDULE — USER AND SERVICE DATA

The following retention periods are consistent with the Corporation's published Privacy Policy. In the event of any conflict between this Policy and the Privacy Policy, the Privacy Policy shall govern with respect to user data handling.

Data Type	Retention Period	Notes
Account information (email, display name)	Until account deletion	Permanently deleted immediately upon account deletion
Trip plan data	Until trip closed + 30 days	Allows post-trip review
Location history	Trip close + 7 days	Deleted automatically
Medical notes	Trip close + 30 days	Encrypted at rest (AES-256-GCM)
Check-in records	90 days	

Data Type	Retention Period	Notes
Alert logs	90 days	
Raw device payloads	30 days	Encrypted at rest
Emergency contact information	Linked to associated trip plan retention	Deleted with associated trip data
Communications (SMS and satellite messages)	Linked to trip record retention	
Audit and access logs	1 year	Security and incident investigation
Backup copies of user data	30 days beyond primary record deletion	Backups purged on rolling basis

8.1 User Deletion Requests. Requests from users to delete their personal information under applicable privacy law (including GDPR, CCPA, and CPRA) shall be processed promptly and in all events within the timeframes specified in the Privacy Policy. Deletion shall be complete across both primary systems and backups, subject to the rolling backup purge schedule stated above.

9. RETENTION SCHEDULE — ELECTRONIC COMMUNICATIONS AND BUSINESS RECORDS

Record Type	Retention Period
Email containing substantive business content	7 years
Routine administrative email	1 year
Calendar entries	3 years
Internal messaging and chat records	1 year
Website content (current production)	Ongoing
Website content archives (superseded versions)	3 years
Social media posts and associated content	3 years
Newsletter archives	Permanent

10. DESTRUCTION PROCEDURES

10.1 Authorization. Records shall be destroyed only after the applicable retention period has expired and no legal hold is in effect.

10.2 Paper Records. Paper records containing confidential or sensitive information shall be destroyed by cross-cut shredding or a comparably secure method. Non-sensitive paper records may be recycled.

10.3 Electronic Records. Electronic records shall be deleted from primary systems and backups using methods appropriate to the sensitivity of the data. Sensitive data (including medical notes, raw device payloads, and user location history) shall be securely wiped in accordance with industry practice.

10.4 Encrypted Data. For data encrypted at rest, secure deletion may be achieved through cryptographic erasure (destruction of encryption keys) in addition to data removal.

10.5 Third-Party Service Providers. The Corporation shall ensure that third-party service providers handling Corporation records follow comparable retention and destruction practices, and shall confirm destruction upon termination of the service relationship.

10.6 Certificate of Destruction. Where appropriate, a record of destruction shall be maintained, including the type of records destroyed, the date of destruction, and the method used.

11. LITIGATION HOLD

11.1 Suspension of Destruction. In the event the Corporation is served with, or reasonably anticipates, any subpoena, discovery request, government investigation, or litigation, the Policy Administrator, in consultation with legal counsel, shall immediately issue a written litigation hold. The hold shall suspend destruction of all potentially relevant records until the hold is lifted.

11.2 Notification. The Policy Administrator shall notify all directors, officers, employees, volunteers, and contractors who may possess relevant records of the litigation hold and their obligation to preserve those records.

11.3 Release of Hold. A litigation hold shall remain in effect until released in writing by the Policy Administrator in consultation with legal counsel.

12. WHISTLEBLOWER PROTECTION

The Corporation maintains a separate Whistleblower Policy, adopted by the Board, which protects directors, officers, employees, volunteers, and contractors who in good faith report suspected violations of law, this Policy, or other Corporation policies, including those who refuse to destroy or alter records in violation of this Policy or applicable law. Reports and protections under this Policy are governed by the Whistleblower Policy in all respects.

13. POLICY AMENDMENT

This Policy may be amended by a majority vote of the Board at any regular or special meeting.

CERTIFICATION

Adopted by the Board of Directors of TrekFreely on 6/21/2026.



Kerry Taylor, Secretary