

Chesapeake Bay Trust Data Privacy Policy

Policy Number: IT-001-001

Policy Owner: Vice President of Finance and Administration

Approved By: President

Effective Date: July 1, 2026

Review Cycle: Annually

1. Purpose

The purpose of this Policy is to protect the privacy of individuals by establishing requirements governing the disclosure, use, sale, and redisclosure of personal information and geolocation data maintained, collected, or provided by the Chesapeake Bay Trust (Trust).

This Policy is intended to comply with Maryland State Government Article §10-1702.

2. Scope

This Policy applies to:

- All Trust employees, contractors, consultants, volunteers, and others acting on behalf of the Trust.
- All personal information and geolocation data collected and maintained by the Trust.
- All disclosures of data to external parties, including vendors, researchers, contractors, governmental entities, auditors, and members of the public.

3. Definitions

Personal Information

Information about an identifiable individual maintained by the Trust, as defined under applicable Maryland law.

In this section, “personal record” or “personal information” means a public record that names or, with reasonable certainty, otherwise identifies an individual by an identifying factor such as:

- (1) an address;
- (2) a description;
- (3) a fingerprint or voice print;
- (4) a number; or
- (5) a picture.

Geolocation Data

Information capable of identifying the physical location or movement of an individual, device, vehicle, or asset.

Sensitive Data

Data that may pose heightened privacy risks, including:

- Precise geolocation information
- Genetic information
- Biometric information
- Health information
- Financial information
- Information concerning minors

Data Recipient

Any person or organization receiving personal information or geolocation data from the Trust.

Redisclosure

The sharing, transfer, licensing, publication, release, or dissemination of information received from the Trust to another person or organization.

Sale

The exchange of personal information or geolocation data for monetary or other valuable consideration.

4. Policy Statement

The Chesapeake Bay Trust is committed to protecting the privacy of individuals whose information is collected through our grantmaking, donor engagement, volunteer programs, educational initiatives, and business operations.

Consistent with Maryland State Government Article §10-1702, the Trust does not sell or personal information to data brokers or other third parties for commercial purposes. We also prohibit contractors, vendors, and service providers acting on the Trust's behalf from selling, licensing, monetizing, or otherwise using personal information for purposes unrelated to the services they provide to the Trust.

The Trust collects only information reasonably necessary to administer its programs and operations. Such information may include names, mailing addresses, email addresses, telephone numbers, organizational affiliations, grant application materials, donor records, and other information voluntarily provided to the Trust.

Personal information collected by the Trust may be shared with employees, contractors, reviewers, auditors, governmental entities, or service providers when necessary to carry out authorized Trust business, comply with legal requirements, administer grants, process donations, conduct program evaluation, or protect the Trust's legal interests.

The Trust does not knowingly disclose personal information for secondary commercial use. Personal information provided to the Trust may not be used by recipients for unrelated marketing, solicitation, data aggregation, resale, or other commercial purposes. The Trust takes reasonable administrative, technical, and physical measures to protect personal information and any sensitive data in its possession, including geolocation information when collected. The Trust seeks to minimize collection of sensitive data and limits access to individuals who have a legitimate business need to access it.

Questions regarding this policy may be directed to:

Chesapeake Bay Trust

108 Severn Avenue

Annapolis, Maryland 21403

www.cbtrust.org

Procedure for Personal Information, Sensitive Data & Redisclosure

1. Purpose

Chesapeake Bay Trust will protect personal information and sensitive data that it receives, maintains, or provides to another party and will prevent unauthorized sale, redisclosure, or secondary use of such information (unrelated to operational purpose).

These procedures are designed to be consistent with Maryland State Government Article §10-1702 and related Maryland privacy requirements. Maryland §10-1702 specifically identifies risks from data brokers, secondary uses, geolocation and other sensitive data, and secondary commercial markets.

2. What employees must do

Before sharing personal or sensitive information outside of the Trust:

- A. Know what you are sharing.**
 - Identify the information.
 - Determine whether it contains personally identifiable, sensitive, geolocation, financial, health, demographic, or other protected information.
- B. Know why you are sharing it.**
 - Confirm the legitimate program, grant, contractual, legal, or operational purpose.
 - Do not use information for a new or unrelated purpose without review.
- C. Share the minimum necessary.**
 - Do not provide an entire database when a report or limited data set will accomplish the purpose.
 - Use aggregate or de-identified information whenever practical.
- D. Know who is receiving it.**
 - Identify the data recipient.
 - Identify a secure means of data transfer.
 - Determine whether the recipient will use subcontractors or other third parties.
 - Do not provide information to a data broker or similar commercial data intermediary without prior approval.
- E. Check the contract.**
 - The agreement must restrict unauthorized use, sale, and redisclosure.
 - Subcontractors must be subject to equivalent restrictions.
- F. Get approval from VP Finance and Administration prior to sharing personal information or sensitive data.**
- G. Document the disclosure.**

Keep the approval, agreement, description of information, purpose, recipient, method of data transfer, and applicable restrictions.

3. Never

Employees and contractors may not:

- Sell personal or sensitive information without express authorization;
- Provide information to a data broker for commercial purposes without approval;
- Allow a vendor to sell or redisclose Trust information;
- Use information for an unrelated purpose;
- Upload confidential personal information into an unapproved AI or public technology platform;
- Provide more information than necessary; or
- Circumvent contractual or privacy restrictions through a third party.

4. If something goes wrong

Immediately notify the **VP of Finance and Administration, IT and the responsible department VP** if you discover that sensitive data has been:

- Sent to the wrong person;
- Accessed without authorization;
- Used for an unauthorized purpose;
- Sold or redisclosed;
- Uploaded to an unauthorized system; or
- Lost or exposed.

Do **not** attempt to conceal, delete, or independently investigate the incident before notifying the VP of Finance and Administration, IT and the responsible department VP.

5. Annual review

IT/ Administration will annually review data sharing policies and related documents.

6. Contract Provision

The Trust will include a standard provision in its agreements to provide for acknowledgement that sensitive data may be received or accessed but is confidential and shall not be disclosed without express written approval.