

PUBLIC PROCEDURES ON THE PROHIBITION OF THE SALE AND REDISCLASURE OF PERSONAL RECORDS & GEOLOCATION DATA

Statutory Compliance Web Publication: *In compliance with Md. Code Ann., State Government Article § 10-1702 (enacted under the Maryland Values Act), the Maryland Center for School Safety (MCSS) has developed and published these official procedures to prevent the sale, monetization, or harmful commercial redisclosure of any personal records or geolocation data provided to or maintained by our agency. MCSS is an independent, public safety unit of State government and does not sell, license, rent, or otherwise commercialize any personal or student records under any circumstances.*

I. POLICY RESTRICTING SALE OR REDISCLOSURE OF PERSONAL INFORMATION

1. Purpose

This policy establishes the mandatory procedural, administrative, and contractual safeguards required to strictly prohibit the sale, commercialization, monetization, or unauthorized redisclosure of State-owned Personal Information (PI) and geolocation data under the control of the Maryland Center for School Safety (MCSS). This policy is developed to ensure absolute compliance with Md. Code Ann., State Government Article § 10-1702 (Maryland Data Privacy and Protection Act of 2026) and DoIT Cybersecurity & Privacy Standard 315-10.

2. Scope

This policy applies directly to all branches, divisions, and operational units of the MCSS. It covers all MCSS employees (including SRO/SSE Training staff, Regional Managers, Data Analysts, and Administrators), contractual staff, and any nonaffiliated third parties who are authorized to collect, store, process, access, or

MARYLAND CENTER for SCHOOL SAFETY

handle Personal Information (PI) on behalf of MCSS.

This policy governs all MCSS-managed or vendor-hosted information systems, databases, Software-as-a-Service (SaaS) platforms, and public-facing portals. It covers all classifications of data, specifically focusing on protecting Level 3 (Confidential) Personal Information (such as student files, training rosters, and PII) and Level 4 (Restricted) Sensitive Data (including precise geolocation metadata pinpointing tipline users within a 1,750-foot radius).

3. Definitions of Roles & Responsibilities

Agency Privacy Officer (APO)

The APO serves as the primary coordinator and director of the MCSS privacy compliance program. Core responsibilities include:

- Determines and documents the specific statutory, regulatory, or grant-based legal authority permitting MCSS to process personal records in consultation with the Assistant Attorney General (AAG) who acts as legal counsel to MCSS.
- Customizes, publishes, and reviews the agency's public Privacy Notice and Data Protection Policies at least annually.
- Leads the privacy incident management and breach risk analysis process.
- Maintains the mandated annual Personal Information Data Inventory and submits it to DoIT's Office of Enterprise Data (OED).
- Collaborates with GRC, IT, and Procurement staff to vet and execute vendor Data Use Agreements (Attachment Y).

Procurement Officer (PO) & Contract Monitor (PCM)

The PO & PCM oversee contractual privacy terms and third-party vendor compliance during the acquisition and contract lifecycle. Core responsibilities include:

- Ensures the mandatory execution of the state-approved Attachment Y: Data Use Agreement (DUA) as an integrated part of all new, renewed, or modified contracts where a vendor processes MCSS personal records.
- Verifies and defines the exact data elements the vendor is authorized to access using the Appendix A Checklist, ensuring only the minimum necessary data is shared.
- Ensures contract modifications are signed if the scope of the vendor's data processing elements changes.
- Maintains the vendor's current Appendix B (Sub-processor Directory) to track and monitor downstream data access.

MARYLAND CENTER for SCHOOL SAFETY

- Ensures vendors return or destroy all MCSS records upon contract termination and file a completed, witnessed Appendix C: Certificate of Data Destruction.

Agency Data Owner (DO) / Data Analyst

The DO and Data Analyst act as custodians of the operational datasets, safety statistics, and database systems. Core responsibilities include:

- Enforces the principle of data minimization at the database and application levels, ensuring fields are restricted to only what is necessary for a specific, legitimate school safety purpose.
- Under the direction of the APO, manages role-based access control (RBAC) to ensure only authorized MCSS staff have 'need-to-know' access to sensitive student or SRO records.
- Applies privacy-enhancing technologies (PETs) and de-identification/aggregation methods (such as MSDE suppression rules) to ensure public-facing statistical reports contain no individual-level PII or precise geolocation coordinates.

Governance, Risk, and Compliance (GRC) / Cybersecurity Designee (CISO)

The GRC Designee and CISO audit system security, identify technology risks, and monitor third-party processor systems. Core responsibilities include:

- Performs technical third-party risk assessments and periodic compliance audits to verify that MCSS vendors are not monetizing data or repurposing records for non-contractual uses.
- Conducts formal Privacy Impact Assessments (PIAs) and Algorithmic Impact Assessments (AIAs) for any high-risk system or AI software procurement that processes Level 3 or Level 4 data.
- Maintains the central technical ledger identifying and classifying all MCSS systems containing personal records.

Records Custodian (RC) / Public Information Officer (PIO)

The Records Custodian and PIO review public-facing document releases and manage individual record correction requests. Core responsibilities include:

- Evaluates bulk data or Public Information Act (PIA) requests, denying the release of individual-level personal records unless explicitly mandated by law.
- Establishes and manages the official, auditable pathway under Md. Code Ann., General Provisions Article § 4-502 for citizens to request corrections or updates to their processed personal records.

MARYLAND CENTER for SCHOOL SAFETY

II. CONTRACTUAL PROHIBITIONS AND PROCUREMENT CONTROLS (SOP Section PT-9.01)

To ensure that external technology vendors, cloud hosts, and software developers operating on behalf of MCSS adhere to the rigorous requirements of Md. Code Ann., State Government Article § 10-1702, MCSS enforces the following mandatory standard operating procedures:

- **Mandatory Data Use Agreements (Attachment Y):** The MCSS Procurement Officer and Contract Monitor, in coordination with the Agency Privacy Officer (APO), ensure that the State-approved Data Use Agreement (Attachment Y) is fully executed and incorporated into all third-party contracts involving the processing, transmission, or storage of personal information.
- **Strict Commercial Use Prohibitions:** All third-party processors authorized to handle data on behalf of MCSS are strictly prohibited from selling, licensing, renting, or resharing personal records. A third-party processor is legally barred from deriving commercial value from State-provided data, including an absolute ban on using agency data for commercial behavioral profiling, targeted or behavioral advertising, or training proprietary machine learning and Generative AI models.
- **Third-Party Risk Auditing:** The Governance, Compliance, and Risk (GRC) designee assigned to perform third-party risk assessments conducts periodic privacy audits to verify that external partners do not repurpose personal records or sensitive data elements for secondary, non-contracted uses, and that proper security safeguards are enforced.
- **Mandatory Data Destruction:** Upon contract completion, expiration, or termination, third-party processors are legally required to securely return or destroy all personal records in their possession. To verify compliance, the vendor must execute and submit a formally witnessed Certificate of Data Destruction (Appendix C to the DUA) to the MCSS APO.

III. PROTECTING PERSONAL RECORDS IN PUBLIC INFORMATION ACT REQUESTS (SOP Section PT-9.01.02)

MCSS complies with the Maryland Public Information Act (MPIA) to maintain government transparency. MCSS actively applies the Fair Information Practice Principles (FIPPs) to protect the privacy of individuals. The MCSS Records Custodian and Agency Data Owner enforce the following standards when administering public records requests:

- **Field-Level Data Minimization:** When responding to a MPIA request, MCSS makes data minimization determinations at the field level, not the record level. A public

MARYLAND CENTER for SCHOOL SAFETY

record will not be withheld in its entirety if specific, legally protected identifying fields can be safely redacted.

- **Prioritization of Aggregate Data:** To mitigate the risk of unauthorized redisclosure of Personal Information, MCSS prioritizes the sharing of fully de-identified, anonymized, or aggregated statistical data over individual-level student or staff records in all public reporting.
- **Statutory Minimization Citations:** When MCSS minimizes or redacts identifying fields in a records release, the Records Custodian formally documents the basis of the minimization in the written agency response, explicitly citing DoIT Standard 315 and Md. Code Ann., State Government Article § 10-1702.
- **Discouraging Bulk Records Releases:** Bulk information requests seeking large-scale personal records are actively discouraged. If legally permissible under the MPIA, the Records Custodian will enforce strict field-level redactions to prevent commercial data brokers from exploiting public files to establish secondary commercial markets.

IV. GEOLOCATION AND PERSONAL RECORD SAFEGUARDS BY MCSS PROGRAM AREA

MCSS Program & System	Geolocation & Personal Record Safeguards
Safe Schools Maryland (SSMD) Anonymous Reporting System	SSMD is available 24/7/365 to report school and student safety concerns. In compliance with Protection of Information by Government Agencies Act (PIGA) and Md. Code Ann., State Government Article § 10-1702, MCSS does not collect or store precise geolocation data (within a 1,750-foot radius) from users of our mobile apps or website portals without explicit consent, and never shares or sells this data. Tip information is restricted to active school safety emergency responders on a strict need-to-know basis. Pursuant to Md. Code Ann., Gen. Provis. §4-314.1, information and materials related to SSMD is exempt from disclosure.
School Resource Officer (SRO) & Security Portal	The portal tracks mandated training, SRO coverage grant allocations, and official security rosters. Personal and professional credentials of security personnel are classified

MARYLAND CENTER for SCHOOL SAFETY

as protected personal records. MCSS enforces Zero Trust¹ access controls on these databases and strictly prohibits vendors from utilizing SRO registration lists for commercial mailing, marketing, or promotional purposes.

V. CONTACT AND INQUIRIES

For any questions regarding MCSS data privacy practices, agency compliance with Md. Code Ann., State Government Article § 10-1702, or to exercise your rights under the Maryland Public Information Act regarding records correction, please contact the MCSS Agency Privacy Officer directly:

Title / Role: Agency Privacy Officer (APO)
Agency: Maryland Center for School Safety (MCSS)
Address: 200 W. Baltimore Street, Baltimore, MD 21201
Main phone: 410-281-2335
Dedicated Email: privacy.mcass@maryland.gov

¹ In compliance with DoIT Cybersecurity Standards and CJIS, MCSS is actively transitioning core database systems and safety portals to a Zero Trust Architecture (ZTA) operating on the principle of 'never trust, always verify.'