

MARYLAND CENTER for SCHOOL SAFETY

Agency Data Privacy Policy & Governance

Effective/Issue Date: October 1, 2026	Reviewed Date: September 2026
Revised Date: October 1, 2026	Index Number: Policy 400.03

Overview & Purpose

Overview: The Maryland Center for School Safety (MCSS) operates as an independent unit of State government established to promote, support, and enhance school communities that are safe for learning and teaching. Because the agency's unique operational scope bridges educational institutions, law enforcement, and other state agencies, MCSS maintains a heightened statutory responsibility to handle all personal records with the highest standards of confidentiality and security.

Purpose: This policy establishes the formal privacy governance framework and mandatory data protection standards required under Maryland State law and applicable Federal regulations. This policy is directly aligned with the Department of Information Technology (DoIT) Data Protection and Privacy Policy (MD-POL-205-01) and the PII and Transparency Standard (MD-STD-315-PT-02) and is enforceable across all agency divisions. This policy completely replaces and supersedes all previous versions of the MCSS Data Privacy Policy. Any prior policies concerning the subject matter herein shall have no further force or effect.

MCSS operates within a multi-layered government privacy framework. This framework translates foundational privacy principles into binding state statutes, technical controls (e.g., encryption and secure storage protocols), and operational oversight to protect personal records across all agency operations.

MARYLAND CENTER for SCHOOL SAFETY

REGULATORY DEADLINE & STATUTORY MANDATE

(MD. STATE GOV'T § 10-1702):

Pursuant to Md. Code Ann., State Government Article § 10-1702(c), MCSS shall maintain, publish, and submit its data privacy policy and governance standards to the Maryland General Assembly (specifically to the Senate President and Speaker of the House). This policy document shall be reviewed, updated, and re-approved at least once every three (3) years.

Definitions & Abbreviations

AAG (Assistant Attorney General): The legal counsel assigned to MCSS by the Maryland Office of the Attorney General, responsible for providing legal guidance, conducting legal sufficiency reviews of agency policies, agreements, and contracts, and advising on statutory privacy compliance, public disclosures, and data breach notifications.

APO (Agency Privacy Officer): The designated MCSS official responsible for leading agency privacy governance, maintaining personal information inventories, conducting privacy risk evaluations, managing privacy incidents, and reviewing privacy notices and agreements.

CIO (Chief Information Officer): The agency executive responsible for overseeing MCSS's information technology infrastructure, technical security baselines, and enterprise data systems, including data inventory tracking, technical containment during security incidents, and operational alignment with the Department of Information Technology (DoIT) and Maryland Coordination and Analysis Center (MCAC) standards.

CJI / CJIS (Criminal Justice Information / CJIS Security Policy): Restricted criminal history records, background checks, and law enforcement data governed by the FBI and Maryland State Police CJIS Security Policy.

Data Minimization: The statutory requirement (MD-STD-315-PT) to collect, process, share, and retain only the minimum necessary personal information required to accomplish an authorized, specified purpose.

MARYLAND CENTER for SCHOOL SAFETY

DoIT: Maryland Department of Information Technology.

DSA (Data Sharing Agreement): A formal administrative data governance agreement executed between MCSS and other units of State government, local government entities, school systems, or academic research institutions. A DSA defines the authorized operational purpose, field-level dataset restrictions, security controls, and handling protocols for shared records containing Personal Information (PI). A DSA works directly in tandem with a Memorandum of Understanding (MOU) or Interagency Agreement (IAA): while the MOU establishes the overarching administrative partnership, operational scope, and service commitments between the agencies, the DSA serves as the dedicated data governance framework defining data stewardship and privacy baselines for the exchanged dataset.

DUA (Data Use Agreement/Attachment Y): A mandatory contractual addendum required for third-party vendors and contractors that access, process, host, or collect MCSS personal records. Required under Maryland procurement law and DoIT standards, it establishes binding security controls, strictly prohibits the sale or commercialization of state data, and mandates one-business-day breach notification and certified data destruction.

Exigent Threat / Active Emergency Situation: An active, articulable, and imminent threat to the life, health, or physical safety of students, staff, or school community members. An exigent threat legally triggers authorized emergency exceptions under FERPA (34 CFR § 99.36), HIPAA (45 CFR § 164.512(j)), CJIS Security Policy (§ 5.3), and Md. Code Ann., Educ. Article § 7-1502, authorizing MCSS personnel to immediately receive and disclose necessary identifiable personal records to active first responders and law enforcement dispatch without prior consent.

Media Sanitization: The administrative and technical process of irreversibly removing, overwriting, or physically destroying data stored on physical or digital media (e.g., hard drives, mobile devices, flash drives, backup tapes) prior to disposal, reuse, or decommissioning, in strict accordance with **NIST SP 800-88 Rev. 1** standards and DoIT security policies so that data recovery is impossible.

Need-to-Know Access: The foundational access control principle restricting dataset, repository, or physical record access strictly to authorized personnel who require specific personal records to perform legitimate, documented

MARYLAND CENTER for SCHOOL SAFETY

government job duties. Access is governed by Role-Based Access Control (RBAC) and system access logs.

Non-Exigent / Standard Safety Operations: Routine, non-emergency school safety functions—including general technical assistance, policy reviews, SRO/SSE training administration, and non-emergency behavioral threat assessment (BTA) consultations—where no active, immediate threat to life exists. Non-exigent operations strictly require field-level data minimization, de-identification, and removal of direct.

FERPA: Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99), protecting student education records.

FIPPs (Fair Information Practice Principles): The foundational set of internationally recognized privacy principles (Transparency, Purpose Specification, Use Limitation, Data Minimization, Security Safeguards, Individual Participation, and Accountability) that form the baseline for State and Federal privacy frameworks.

HB 264/Ch_435 (2026): Maryland Data Privacy and Protection Act of 2026 (effective October 1, 2026), expanding sensitive data definitions and commercial restrictions.

MCSS: Maryland Center for School Safety (preferred agency abbreviation).

MD-STD-315-PT-02: The Department of Information Technology PII and Transparency Standard, establishing mandatory administrative, technical, and operational privacy controls for Maryland Executive Branch agencies.

Operational Intermediary: An entity (such as MCSS) that receives, analyzes, or transmits personal records solely to provide specialized consultation, technical assistance, or safety coordination, without serving as the primary legal custodian or central repository for those records. Legal ownership and primary custodial obligations remain with the originating local education agency, health entity, or law enforcement agency.

PIGA: Protection of Information by Government Agencies Act (Md. Code Ann., State Gov't § 10-1301 et seq.).

Personal Information (PI) - State Defined: Under Maryland law (State Gov't §§ 10-1301 and 10-1702), data containing an individual's first name (or initial) and last name combined with a protected element, such as a Social Security

MARYLAND CENTER for SCHOOL SAFETY

Number, driver's license number, financial credential, statutory Sensitive Data, or Precise Geolocation within a 1,750-foot radius. For full statutory breakdown and classification rules, **see Section 5.1.2.1.**

Personally Identifiable Information (PII) - Federal Defined: Information that can directly or indirectly trace or distinguish an individual's identity under Federal statutes, grants, FERPA, or CJIS frameworks. For full statutory breakdown and classification rules, **see Section 5.1.2.2.**

Precise Geolocation: Coordinate-based or digital data derived from technology that can precisely identify physical location within a 1,750-foot radius (Md. Code Ann., Com. Law § 14-4701; State Gov't § 10-1702).

PT / 415-PT (PII & Transparency Procedure Taxonomy): The administrative index code derived from DoIT Standard MD-STD-315-PT and the NIST SP 800-53 (Rev. 5) Privacy Control Domain ("PII Processing and Transparency"). In MCSS governance, "PT" designates operational standard operating procedures governing Personally Identifiable Information (PII) processing, data minimization controls, public transparency notices, Privacy Threshold Analyses (PTAs), and Privacy Impact Assessments (PIAs).

Purpose Limitation (Purpose Specification / Use Limitation): The Fair Information Practice Principles (FIPPs) and statutory mandate (DoIT MD-STD-315-PT-02, PT-2/PT-3) require MCSS to explicitly document and disclose the authorized government purpose for collecting personal information prior to or at the time of collection. This principle strictly restricts subsequent processing, sharing, or vendor handling to that specified purpose, prohibiting unauthorized secondary uses, commercial repurposing, or profiling.

Software as a Service (SaaS) Vendor: An external contractor or technology provider that delivers cloud-hosted software applications, web portals, or digital data collection tools accessed over the internet. Any SaaS vendor that receives, hosts, stores, or processes State Personal Information (PI), PII, or sensitive safety data on behalf of MCSS is classified as a Third-Party Data Processor and is legally subject to mandatory Attachment Y Data Use Agreement (DUA) execution, field-level data minimization (Appendix A), sub-processor oversight (Appendix B), and certified data destruction (Appendix C) under **DoIT MD-STD-315-PT (PT-10) and Md. Code Ann., State Gov't § 10-1702.**

MARYLAND CENTER for SCHOOL SAFETY

Statutory Sensitive Data (Sensitive Data): Highly protected categories of Personal Information defined under House Bill 264 (Md. Code Ann., State Gov't §§ 10-1301 and 10-1702; Com. Law § 14-4701), including data revealing racial or ethnic origin, religious beliefs, health data, sexual orientation, transgender or nonbinary status, citizenship or immigration status, genetic or biometric data, personal data of a child under 18, or precise geolocation.

Core Framework of Agency Data Privacy Policy & Governance

Why These Reference Sections Matter

While this policy sets our day-to-day privacy rules, it cannot predict every unique situation, new technology, or special safety case. Sections 1 through 3 below serve two main purposes:

- **For MCSS Staff (Handling Edge Cases):** If MCSS staff encounter a situation or new software not explicitly covered in this policy, use these core principles, especially **Data Minimization** and **Purpose Limitation**, as your decision-making guide, and consult with the APO and CIO before collecting or sharing data.
- **For Policy Updates (Continuous Compliance):** These sections highlight the specific state laws, IT standards, and national privacy frameworks that the APO monitors to keep MCSS compliant and guide future updates to this policy (policy updated once every three years per Md. Code Ann., State Gov't § 10-1702 (HB 264)).

1. Core Principles: Fair Information Practice Principles (FIPPs)

The agency's privacy governance is anchored in the eight Fair Information Practice Principles (FIPPs), establishing the baseline standard for handling personal records:

- 1.1. **Transparency:** Publishing clear, accessible privacy notices informing individuals about data collection and processing activities.

MARYLAND CENTER for SCHOOL SAFETY

- 1.2. **Purpose Specification:** Documenting explicit legal authority and specified government purposes prior to data collection.
- 1.3. **Use Limitation:** Restricting processing strictly to consented, authorized uses; prohibiting commercial sales, monetization, and profiling.
- 1.4. **Data Minimization:** Requesting and retaining only the absolute minimum personal information necessary to accomplish authorized tasks.
- 1.5. **Security Safeguards:** Administering technical, physical, and administrative controls to protect data throughout its lifecycle.
- 1.6. **Data Quality & Integrity:** Maintaining accurate, relevant, and timely records.
- 1.7. **Individual Participation:** Supporting individual rights of access, inspection, and administrative correction under state law.
- 1.8. **Accountability & Audit:** Enforcing internal privacy roles, staff training, routine compliance reviews, and mandatory logs.

MCSS personnel shall operationalize the Fair Information Practice Principles (FIPPs), public notice disclosures, and foundational privacy compliance in accordance with the administrative workflows detailed in **MCSS SOP-415-PT Section PT-1.0**.

2. Legal & Regulatory Governance

MCSS operations adhere strictly to overlapping state and federal statutory requirements:

- 2.1. **Maryland Protection of Information by Government Agencies Act (PIGA) & HB 264/Ch. 435 (2026):** Governs state agency personal records, restricts the commercialization of data, and establishes heightened protections for statutory Sensitive Data and Precise Geolocation (within a 1,750-foot radius).
- 2.2. **Health Insurance Portability and Accountability Act (HIPAA):** (42 U.S.C. § 1320d et seq.; 45 CFR Parts 160 and 164) Protects individually identifiable health information (PHI). When MCSS processes, stores, or transfers medical records or health alerts, the

MARYLAND CENTER for SCHOOL SAFETY

agency enforces HIPAA-compliant safeguards. Where HIPAA rules are more stringent than State policy, HIPAA rules take precedence.

- 2.3. **Family Educational Rights and Privacy Act (FERPA):** (20 U.S.C. § 1232g; 34 CFR Part 99) Protects student education records and limits disclosures to specific statutory safety exceptions (such as school officials, law enforcement unit records, health and safety emergencies, or juvenile justice information sharing).
- 2.4. **Criminal Justice Information Services (CJIS) Security Policy:** Governs the protection, handling, and access auditing of restricted criminal history records and law enforcement database queries.
- 2.5. **Maryland Online Data Privacy Act (MODPA):** (Md. Code Ann., Com. Law § 14-4701) Serves as the state's commercial privacy reference standard for non-governmental vendor practices.

MCSS personnel shall apply these governance definitions during project planning, contract drafting, and interagency collaboration in accordance with the classification and review workflows detailed in **MCSS SOP-415-PT Section PT-2.0**.

3. Privacy Program Management & Technical Implementation

Technical controls and administrative workflows are operationalized through state mandates and national standards:

- 3.1. **NIST Framework Alignment:** (Md. Code Ann., State Fin. & Proc. § 13-115) Technical architectures are built to conform with the NIST Privacy Framework V1, NIST SP 800-53 Rev. 5 (Security & Privacy Controls), NIST SP 800-207 (Zero Trust Architecture), and NIST SP 800-88 (Guidelines for Media Sanitization).
- 3.2. **DoIT Policy Baseline:** System compliance is governed by Department of Information Technology standards, including MD-POL-205-01 (Data Protection & Privacy Policy) and MD-STD-315-PT (PII & Transparency Standard).

MARYLAND CENTER for SCHOOL SAFETY

MCSS personnel shall operationalize these statutory requirements, FIPPs principles, and technical standards in accordance with the intake checklists and verification workflows detailed in **MCSS SOP-415-PT Section PT-1.0 through PT-3.0.**

4. Agency Roles & Responsibilities

MCSS IT administrators, system custodians, and GRC personnel shall execute Zero Trust network configuration, FIPS 140-3 encryption verification, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Privacy Threshold Analyses (PTA) / Privacy Impact Assessments (PIA) in accordance with the technical workflows detailed in MCSS SOP-415-PT Section PT-3.0.

Designated Role	NIST Control Alignment	Core Operational Responsibilities
Agency Privacy Officer (APO)	PT-2.01, PT-3.01, PT-4.01, PT-5.01, PT-7.01, PT-9.01	Leads agency privacy governance. Documents legal processing authority in coordination with SCPO and AAG. Performs annual personal information inventories, manages privacy breaches, reviews website notices, and signs off on DUAs.

MARYLAND CENTER for SCHOOL SAFETY

Designated Role	NIST Control Alignment	Core Operational Responsibilities
Governance, Risk & Compliance (GRC) <i>Collective function, not a specific role. Joint MCSS–DoIT Model (APO, CIO & Procurement, supported by DoIT OSM)</i>	PT-2.01, PT-3.01, PT-7.01, PT-9.01, PT-10.01	Executes system risk reviews, technical privacy impact assessments (PIAs), and Zero Trust security audits. Note for Staff: This function is administered jointly with DoIT. All day-to-day staff GRC inquiries, PIA forms, and vendor privacy reviews must be submitted directly to the Agency Privacy Officer (APO)
Agency Data Owner (DO)	PT-3.01, PT-9.01.01	Maintains direct custody over specific datasets (e.g., Safe Schools Maryland database). Restricts data processing to compatible, authorized agency purposes. Enforces strict need-to-know access criteria.

MARYLAND CENTER for SCHOOL SAFETY

Designated Role	NIST Control Alignment	Core Operational Responsibilities
Procurement Contract Monitor	PT-3.01, PT-9.01, PT-10.01	Ensures a State-approved Data Use Agreement (Attachment Y) is executed for every contract involving personal information processing. Monitors compliance with DUA Appendix A data elements.
Records Custodian & PIO	PT-9.01.01	Manages compliance with the Maryland Public Information Act (MPIA). Implements Fair Information Practice Principles (FIPPs) during public record requests. Enforces field-level data minimization.

5. Operational Privacy Standards

This section establishes mandatory agency-wide operational standards governing data classification, purpose specification, and data minimization across all MCSS systems and safety programs.

5.1. Purpose Specification & Data Scope

5.1.1. Purpose Specification & Use Limitation Baseline: Under FIPPs Use Limitation and DoIT Standard MD-STD-315-PT, the precise purposes for which Personal Information (PI) or Personally Identifiable Information (PII) is collected must be documented and specified at or before the time of

MARYLAND CENTER for SCHOOL SAFETY

collection. Subsequent processing, sharing, or vendor handling is strictly restricted to that specified, authorized purpose or to purposes formally deemed compatible by the Agency Privacy Officer (APO) and legal counsel. Unauthorized secondary processing, data sales, monetization, and commercial profiling are strictly prohibited.

5.1.2. **Statutory Data Scope & Classification Standards**

(Maryland PI vs. Federal PII): MCSS personnel shall distinguish between State-Defined Personal Information (PI) under Maryland law (Md. Code Ann., State Gov't §§ 10-1301 and 10-1702) and Federal Personally Identifiable Information (PII) under Federal regulations (FERPA, CJIS, NIST SP 800-60). Personnel shall classify agency datasets according to their governing statutory definitions and apply required administrative, technical, and physical safeguards prior to data intake, system onboarding, or external transmission.

5.1.2.1. **State-Defined Personal Information (PI) [Md. Code Ann., State Gov't §§ 10-1301 and 10-1702; HB 264]:**

State Personal Information constitutes any dataset containing an individual's first name (or first initial) and last name in combination with one or more of the protected elements, sensitive attributes, or location metrics listed below. Exposure or processing of State PI triggers mandatory State compliance mechanisms, including Attachment Y Data Use Agreements (DUAs) for third-party contractors, Privacy Impact Assessments (PIAs), annual reporting in the MCSS Personal Information Data Inventory, and formal State breach notification protocols under PIGA:

- 5.1.2.1.1. **Government Identifiers:** Social Security Number (SSN), Individual Taxpayer Identification Number (ITIN), Passport Number,

MARYLAND CENTER for SCHOOL SAFETY

Driver's License Number, or State Identification Card Number.

- 5.1.2.1.2. **Financial Credentials:** Financial, bank, or credit/debit card account numbers that, in combination with any required security code, access code, or password, permit access to an individual's financial account.
- 5.1.2.1.3. **Account Logins & Security Credentials:** A username or email address combined with a password, PIN, or security question and answer that permits access to an individual's account.
- 5.1.2.1.4. **Statutory Sensitive Data (Protected Class Data):** Personal data revealing:
 - 5.1.2.1.4.1. Racial or ethnic origin, or religious beliefs;
 - 5.1.2.1.4.2. Consumer health data, protected health information (PHI), mental health, substance use disorder, or disability status;
 - 5.1.2.1.4.3. Sex life, sexual orientation, or status as transgender or nonbinary;
 - 5.1.2.1.4.4. National origin, citizenship, or immigration status;
 - 5.1.2.1.4.5. Genetic data or unique biometric print/image (e.g., fingerprints, facial geometry);
 - 5.1.2.1.4.6. Personal data of an individual that MCSS knows, or has reason to know, is a child under 18 years of age; or
 - 5.1.2.1.4.7. Inferred Sensitive Data (information deduced or calculated from surrounding data elements that indicates protected class status).

MARYLAND CENTER for SCHOOL SAFETY

- 5.1.2.1.5. **Precise Geolocation Data:** Coordinate-based or digital location data derived from technology (e.g., mobile devices, tipline applications, or vehicles) capable of identifying the physical location of an individual or device within a 1,750-foot radius.
- 5.1.2.2. **Federal Personally Identifiable Information (PII) [FERPA 34 CFR § 99.3; CJIS Security Policy § 4.3; OMB M-03-22]** Federal Personally Identifiable Information encompasses any information that can directly or indirectly trace, distinguish, or identify an individual alone or when combined with other personal or identifying details linked or linkable to a specific individual:
 - 5.1.2.2.1. **Direct Identifiers:** Standalone details that identify a specific person, including full names, personal phone numbers, personal email addresses, home addresses, or State Assigned Student Identifiers (SASIDs).
 - 5.1.2.2.2. **Indirect / Linkable Identifiers:** Information that does not name an individual directly but permits identification when combined with contextual data, including dates of birth, place of birth, mother's maiden name, SRO background files, or tipline case numbers.
 - 5.1.2.2.3. **Student Education Records (FERPA):** Any record directly related to a student and maintained by an educational agency/institution (LEA) or a party acting for the agency/institution. Standing alone, student contact details or demographic files constitute PII under FERPA and require strict adherence to authorized statutory exceptions prior to disclosure.

MARYLAND CENTER for SCHOOL SAFETY

5.1.3. Work Contact Information vs. Personal Contact Information

- 5.1.3.1. **Work Contact Information:** Official employee names, state/agency work email addresses, work phone numbers, and office addresses are classified as Level 1 (Public) when published on official state websites, or Level 2 (Internal Only) when compiled into internal operational directories.
- 5.1.3.2. **Personal Contact Information:** Non-public personal email addresses, personal phone numbers, or home addresses. Personal contact information does not constitute State PI on its own; however, if personal contact details are collected or stored in combination with a password, PIN, or account security credentials, the dataset automatically escalates to Level 3 (Confidential State PI)—triggering mandatory DUA execution, data inventory tracking, and formal breach notification protocols.

5.2. Strict Definitions: Sensitive Data & Precise Geolocation

House Bill 264 expanded the statutory definition of protected Personal Information to include highly sensitive data categories. Processing these categories requires written legal justification and strict consent protocols:

- 5.2.1. **Racial or Ethnic Origin & Beliefs:** Data revealing racial or ethnic origin, religious beliefs, national origin, or citizenship/immigration status.
- 5.2.2. **Health & Status Identifiers:** Data revealing consumer health conditions, protected health information (PHI), sex life, sexual orientation, or status as transgender or nonbinary.
- 5.2.3. **Biometrics & Genetics:** Unique genetic data, biometric print/image, or physical fingerprints.
- 5.2.4. **Child Data:** Any personal data of an individual that MCSS knows, or has reason to know, is a child under 18 years of age.

MARYLAND CENTER for SCHOOL SAFETY

- 5.2.5. Precise Geolocation Information:** Any coordinate-based or digital data derived from technology that can precisely locate an individual, mobile device, or vehicle within a 1,750-foot radius (such as GPS coordinates or Wi-Fi mapping).

MCSS personnel shall execute statutory authority verifications, purpose specifications, and data classification checks pursuant to the following operational procedures in **MCSS SOP-415-PT**:

- **Section PT-2.01:** Authority to Process PII (Legal Basis Verification)
- **Section PT-3.01:** PII Processing Purposes & Need-to-Know Access Controls
- **Section PT-5.01:** Privacy Disclosures & Data Scope Audits
- **Section PT-7.01:** Specific Categories of PII/PI (State PI vs. Federal PII Classification Rules)

5.3. The Core Principle of Data Minimization

Data minimization is the primary operational defense against unauthorized exposure. MCSS personnel shall collect, process, share, and retain only the absolute minimum amount of personal information necessary to accomplish a legitimate, specified government purpose:

- 5.3.1. Field-Level Determinations:** Data minimization shall be evaluated at the field level, not the record level. If an operational safety report requires a count or trend analysis, personnel shall not collect individual student names, dates of birth, or identification numbers.
- 5.3.2. Limiting Collection of Sensitive Data & Precise Geolocation:** Collection of statutory Sensitive Data (e.g., race, religion, health data, sexual orientation, or immigration status) and Precise Geolocation within a 1,750-foot radius is strictly restricted to authorized school safety functions or explicit statutory mandates.

MARYLAND CENTER for SCHOOL SAFETY

- 5.3.3. Non-Mandated PII Purging:** If a Local Education Agency (LEA), law enforcement partner, or external entity mistakenly submits unrequested or non-mandated PII to MCSS, personnel shall immediately purge the unrequested data fields in accordance with field-level data minimization rules.

MCSS data requestors, custodians, and contract monitors shall enforce field-level data minimization and commercialization prohibitions pursuant to the following operational procedures in **MCSS SOP-415-PT**:

- **Section PT-9.01:** Agency Prohibition on the Sale of Personal Information (SG § 10-1702 Audit Protocol)
- **Section PT-9.01.01:** Field-Level Data Minimization & Non-Mandated PII Purging Protocols
- **Section PT-9.01.02:** FIPPs Compliance, Data Suppression & Aggregation Standards

5.4. Statutory Inventory of Mandated School Safety Data Collections

Pursuant to the Maryland Safe to Learn Act (Md. Code Ann., Educ. §§ 7-1502(g) and 7-1508), House Bill 782 (2025), and DoIT Standard MD-STD-315-PT, MCSS is statutorily authorized to collect, process, and analyze specific school safety datasets necessary to fulfill its legislative mission. In alignment with data minimization mandates, data intake for each collection is strictly limited to authorized fields and mapped to the annual MCSS Personal Information Data Inventory:

- 5.4.1. School Resource Officer (SRO) & Security Employee (SSE) Staffing Rosters:** Annual collection of SRO/SSE assignment data across Maryland public school systems to evaluate coverage and training compliance (Md. Code Ann., Educ. § 7-1508(c)).
- 5.4.2. SRO & SSE Use-of-Force Incident Logs:** Mandated reporting of all use-of-force incidents involving an SRO or

MARYLAND CENTER for SCHOOL SAFETY

SSE and a student while the officer is performing school duties (Md. Code Ann., Educ. § 7-1508(i)).

- 5.4.3. Emergency Plan (EP) Performance Summaries:** Annual submissions from LEAs detailing school emergency drill performance, multi-hazard preparedness, and facility safety evaluations (Md. Code Ann., Educ. § 7-1502(g)).
- 5.4.4. School Safety Evaluation Summaries:** Biennial assessments submitted by local school systems evaluating physical infrastructure, access control, and emergency communication capabilities.
- 5.4.5. Safe Schools Maryland Anonymous Tipline Records:** Intake logs, tip details, and location data collected via app, web portal, and phone intake (1-833-MD-B-SAFE) to analyze threat trends and facilitate immediate emergency dispatch. (Md. Code Ann., Educ. § 7-1514).
- 5.4.6. Specialized School Safety Infrastructure Studies:** Statutory studies analyzing weapon detection technology, security infrastructure, and safety gaps across Maryland public middle and high schools (House Bill 782, 2026).

MCSS personnel handling tipline logs, emergency plans, child data (<18), or precise location records shall execute heightened security controls pursuant to the following operational procedures in **MCSS SOP-415-PT**:

- **Section PT-7.01:** Statutory Sensitive Data Handling, Child Data Safeguards & Precise Geolocation Radius Controls (1,750-ft Limit)
- **Section PT-10.01:** Emergency Health Indicator Safeguards, LEA Intake Verification & Vendor DUAs

6. Operational Safety Intermediary Status & Program-Specific Contexts

In executing its statutory school safety functions under Maryland Education Article § 7-1502, MCSS functions as an operational safety intermediary, analyzing and evaluating school safety data while respecting the primary

MARYLAND CENTER for SCHOOL SAFETY

record ownership and statutory boundaries established under FERPA, CJIS, and State law.

6.1. Institutional Posture & Operational Disclaimer

MCSS operates as an **operational intermediary**. MCSS is not a primary repository for student education records governed by FERPA, protected health records governed by HIPAA, or criminal history records governed by CJIS. Primary record ownership and custodial responsibilities remain with the originating Local Education Agencies (LEAs), healthcare entities, or law enforcement agencies. MCSS collects, receives, and analyzes such records solely to fulfill authorized school safety, threat assessment consultation, and technical assistance functions pursuant to Maryland Education Article § 7-1502.

Public Records Disclosure Exemption for Intermediary Records: Records or record extracts in MCSS's temporary possession that were provided by LEAs, health entities, or law enforcement agencies under statutory exemptions retain their underlying federal and state statutory confidentiality protections. Pursuant to the Maryland Public Information Act (General Provisions Article § 4-301 et seq.) and State Government Article § 10-1702, such records do not become public state records by virtue of being shared with MCSS and remain exempt from public inspection, subpoena, or MPIA disclosure requests.

6.2. Operational Thresholds for Safety Consultations

6.2.1. Non-Exigent Consultations (Standard Operations): For routine technical assistance, safety evaluations, policy reviews, School Resource Officer / School Security Employee (SRO/SSE) training coordination, and non-emergency behavioral threat assessment (BTA) consultations, staff shall enforce strict field-level data minimization. Personnel shall ensure all student or individual identifiers are removed or de-identified prior to intake if communicating through standard channels. Access is restricted strictly on a **Need-to-Know** basis, and secondary redisclosure is prohibited.

MARYLAND CENTER for SCHOOL SAFETY

6.2.2. Exigent Threat Situations (Active Emergencies): In circumstances involving an active, articulable, and imminent threat to the life, health, or safety of students, staff, or school communities, MCSS personnel are statutorily authorized to receive, process, and immediately share identifiable records with active first responders, LEA emergency teams, and law enforcement pursuant to authorized statutory exceptions:

- 6.2.2.1. **FERPA Health & Safety Emergency Exception:** (34 CFR § 99.36 & § 99.31(a)(10)) Permits LEAs to disclose student education records without prior parental consent to appropriate safety and emergency parties during an emergency.
- 6.2.2.2. **HIPAA Serious & Imminent Threat Exception:** (45 CFR § 164.512(j)) Permits healthcare and school medical professionals to disclose protected health information without patient authorization to prevent or lessen a serious and imminent threat.
- 6.2.2.3. **CJIS Emergency Incident Provisions:** (CJIS Security Policy § 5.3) Permits immediate law enforcement information sharing during active emergency responses.
- 6.2.2.4. **Maryland Safe to Learn Act Mandate:** (Md. Code Ann., Educ. § 7-1502(g)) Mandates immediate technical and operational support from MCSS during school safety emergencies.

6.3. LEA Data Transmission, Validation & Emergency Record Controls

6.3.1. Mandatory Secure Intake Channels: All mandated school safety reports, tipline logs, and emergency plan submissions from Local Education Agencies (LEAs) shall occur exclusively through secure, encrypted State intake portals or authorized SaaS platforms in compliance with DoIT Cybersecurity Policy (MD-POL-205-01). All digital data

MARYLAND CENTER for SCHOOL SAFETY

transfers shall enforce transport encryption (TLS 1.2 or higher) and storage encryption at rest (AES-256) utilizing FIPS 140-3 validated cryptographic modules.

- 6.3.2. Intake Validation & Data Integrity:** MCSS shall enforce data validation and quality control standards on all LEA submissions upon receipt to verify record completeness, maintain data integrity, and ensure prompt remediation of data entry errors in coordination with designated LEA data liaisons.

MCSS personnel shall execute consultation de-identification, emergency disclosure logging, tipline data handling, and unsolicited data purging in accordance with the operational workflows detailed in MCSS SOP-415-PT Section PT-6.0.

7. Data Retention & Cryptographic Disposal Standards

This section establishes mandatory agency rules governing record retention lifecycles, litigation hold exceptions, and cryptographic media sanitization to ensure personal records are retained only as long as necessary and disposed of securely.

7.1. Data Retention Principles & Statutory Alignment

MCSS shall retain Personal Information (PI) and Personally Identifiable Information (PII) strictly for the minimum duration necessary to fulfill authorized operational, legislative, or threat assessment functions:

- 7.1.1. Maryland State Archives (MSA) Schedule Compliance:** All agency record retention and disposition actions shall comply with MSA-approved record retention schedules.
- 7.1.2. Data Minimization Purging:** Records that reach the expiration of their statutory mandate or authorized operational utility shall be flagged for routine purging during the annual MCSS Personal Information Data Inventory audit cycle.

MARYLAND CENTER for SCHOOL SAFETY

- 7.1.3. Litigation Hold Exception:** When MCSS receives a formal litigation hold, Maryland Public Information Act (MPIA) appeal, or legal subpoena, relevant records shall be preserved immediately, superseding standard retention purging schedules until legal counsel (MCSS AAG) authorizes release.

7.2. Cryptographic & Physical Media Disposal Standards

All digital and physical media containing PI or PII, whether cloud storage, local servers, backup tapes, mobile devices, or paper records, must be sanitized prior to disposal, reuse, or decommissioning in accordance with NIST SP 800-88 Rev. 1:

- 7.2.1. Digital Storage Media (Clear & Purge):** Electronic media containing sensitive records or PI must undergo cryptographic erasure or multi-pass overwrite sanitization complying with FIPS 140-3 validated cryptographic modules. Standard file deletion or drive formatting is strictly prohibited.
- 7.2.2. Physical & Paper Records (Destroy):** Paper case files, tipline logs, or physical reports containing PI must be destroyed via cross-cut shredding (DIN 66399 Level P-4 or higher) or high-temperature incineration conducted by a state-approved document destruction vendor.

7.3. Disposal Verification & Logging

To maintain auditability under DoIT standards, every media sanitization or physical destruction event must be formally verified and logged. MCSS staff or contracted disposal vendors shall execute a formal Certificate of Destruction detailing the date, media serial numbers, sanitization method used, and authorizing officials. Certificates of Destruction shall be retained by the Agency Privacy Officer (APO) for a minimum of five (5) years.

MCSS personnel shall execute retention schedule audits, legal hold locks, and cryptographic media disposal in accordance with the procedures detailed in MCSS SOP-415-PT Section PT-7.0.

MARYLAND CENTER for SCHOOL SAFETY

8. Vendor & Third-Party Oversight

This section establishes mandatory procurement gatekeeping rules, contract requirements, and vendor accountability standards to protect State personal records processed by third-party contractors, cloud providers, and software vendors.

8.1. Mandatory Attachment Y (Data Use Agreement)

Execution & Legal Gatekeeping

In compliance with Md. Code Ann., State Gov't § 10-1702, DoIT Standard MD-STD-315-PT, and state procurement rules, no third-party contractor, SaaS vendor, or cloud provider shall receive, host, process, or maintain MCSS Personal Information without first executing a binding State-approved Data Use Agreement (Attachment Y):

- 8.1.1.** Procurement Gatekeeping: MCSS procurement staff shall ensure Attachment Y is included in all solicitations, contracts, task orders, and contract renewals involving state data.
- 8.1.2.** APO & AAG Approval: The APO and agency Assistant Attorney General (AAG) must review and approve all vendor-proposed data terms prior to contract execution.
- 8.1.3.** Data Element Minimization (Appendix A): Vendors are permitted to access and process only the minimum necessary data fields explicitly approved and checked in DUA Appendix A. Any expansion of processed data fields requires a formal contract modification and updated Appendix A.
- 8.1.4.** Authorized Sub-Processor Controls (Appendix B): Contractors must maintain an accurate list of authorized sub-processors in DUA Appendix B and enforce flow-down contractual terms no less restrictive than State DUA standards.

MARYLAND CENTER for SCHOOL SAFETY

8.2. Commercialization, AI Training, & Data Mining Prohibitions

Third-party vendors contracting with MCSS are strictly prohibited from selling, leasing, licensing, monetizing, or commercializing State PI, PII, or derivative data. Furthermore, vendors shall not utilize MCSS safety data, tipline logs, or school reports to train commercial artificial intelligence (AI) models, build behavioral profiles, or perform secondary data mining.

8.3. Mandatory Vendor Breach Notification & Financial Liability

Any contractor or vendor hosting or processing MCSS data that discovers or suspects a security incident, unauthorized disclosure, or system breach involving state records must notify the APO and CIO within one (1) business day (24 hours) of discovery. Vendor contracts shall enforce full contractor financial liability for credit monitoring, forensic investigation, and individual notification costs resulting from a vendor-side breach.

8.4. Contract Termination & Certified Data Destruction (Appendix C)

Upon contract termination or expiration, the vendor must immediately cease processing state data and, within thirty (30) calendar days, either securely return all MCSS records in an industry-standard format or cryptographically purge all state data in accordance with NIST SP 800-88 Rev. 1 across primary and backup environments. Compliance must be verified by submitting an executed DUA Appendix C: Certificate of Data Destruction to the APO.

MCSS personnel shall execute vendor management, AI reviews, and procurement controls pursuant to **MCSS SOP-415-PT**:

- **PT-3.01:** PII Processing Purposes (Privacy Impact Assessments for AI & SaaS tools)
- **PT-9.01:** Agency Prohibition on the Sale of Personal Information (Commercialization & monetization ban)

MARYLAND CENTER for SCHOOL SAFETY

- **PT-10.01:** Data Use Agreements & Third-Party Processors (Attachment Y DUAs, sub-processors & certified data destruction)

9. Staff Data Intake, Training & Compliance Enforcement Procedures

This section establishes mandatory agency rules governing staff privacy intake reviews, annual privacy awareness training, and compliance enforcement mechanisms to ensure all MCSS personnel uphold state privacy standards.

9.1. Staff Data Intake & Privacy Compliance Review Mandate

Before collecting, ingesting, or sharing any new personal dataset, or onboarding any new software application, cloud service, or AI tool that processes personal information, MCSS personnel must submit a formal Privacy Compliance Data Intake request to the Agency Privacy Officer (APO) and Chief Information Officer (CIO). Personnel shall not initiate data collection or deploy software without written legal authority clearance and technical privacy approval.

9.2. Mandatory Privacy Awareness & Role-Based Training

9.2.1. Universal Staff Training: All MCSS employees, contractual staff, and intern personnel shall complete mandatory State Data Privacy and Cybersecurity Awareness Training upon hire and annually thereafter (via State Workday or DoIT learning modules).

9.2.2. Specialized Role-Based Training: Personnel who handle or maintain access to Level 3 (Confidential State PI) or Level 4 (Restricted Sensitive Data / CJIS records) shall complete specialized role-based privacy training covering field-level data minimization, FERPA exceptions, and secure data handling prior to receiving system credentials.

MARYLAND CENTER for SCHOOL SAFETY

9.3. Compliance Monitoring & Administrative Sanctions

- 9.3.1. Active Monitoring:** MCSS leadership, the APO, and the CIO shall routinely monitor agency systems, intake portals, and vendor contracts for active compliance with this policy.
- 9.3.2. Enforcement & Sanctions:** Compliance with this policy is a condition of employment and system access. Any unauthorized access, improper disclosure, failure to execute required Data Use Agreements (DUAs), or intentional violation of these privacy rules may result in immediate revocation of system access, administrative sanctions, and formal disciplinary action, up to and including termination of employment, and referral for statutory civil or criminal penalties, where applicable.

MCSS personnel shall execute privacy intake requests, complete role-based training requirements, and report compliance concerns in accordance with the procedures detailed in MCSS SOP-415-PT Section PT-9.0.

References & Statutory Citations

- [Maryland House Bill 264 \(Maryland Data Privacy and Protection Act of 2026\).](#)
- [Maryland State Government Article § 10-1301 et seq. \(Protection of Information by Government Agencies Act - PIGA\).](#)
- [Maryland State Government Article § 10-1702 \(Maryland Online Data Protection Act / HB 1222\).](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\): \(42 U.S.C. § 1320d et seq.; 45 CFR Parts 160 and 164\)](#)
- [Family Educational Rights and Privacy Act \(FERPA\) \(20 U.S.C. § 1232g; 34 CFR Part 99\).](#)
- [FBI & Maryland State Police CJIS Security Policy \(v5.9\).](#)
- [Maryland Department of Information Technology \(DoIT\) PII and Transparency Standard \(MD-STD-315-PT-02\).](#)
- [DoIT Standard Operating Procedures for Privacy Threshold & Impact Assessments \(DoIT-SOP-415-PT\).](#)
- [MCSS Policy 400.01 \(Digital Security\).](#)