MARYLAND STATE DEPARTMENT OF EDUCATION (MSDE)

AGENCY DIRECTIVE (AD)	**NUMBER**: AD 23202-001
SUBJECT: **Data Privacy Policy**	**EFFECTIVE DATE:** January 28, 2023

APPROVED: Mohammed Choudhury _____
Mohammed Choudhury
State Superintendent of Schools
Maryland State Department of Education

Section

1. PURPOSE

1.1 This Data Privacy Policy ("Policy") outlines the responsibility to protect the privacy of Personally Identifiable Information (PII) of residents and the Maryland State Department of Education ("MSDE" or "Agency"), and/or the State of Maryland ("State") in MSDE systems while facilitating appropriate data sharing and analyses.

1.2 This Policy serves as a documented set of guidelines for ensuring that MSDE data and information assets are managed consistently and used properly throughout the data lifecycle.

1.3 This Policy concerns the collection, minimization, use, dissemination, sharing, storage, retention and destruction of PII, including sensitive information, and establishes privacy and governance responsibilities.

2. SPECIAL INSTRUCTION

2.1 This Policy must be approved by the Maryland State Superintendent of Schools.

2.2 All MSDE personnel, including contractors, must sign the Data Privacy Policy Acknowledgement Form and comply with its requirements.

2.3 Relevant portions of this Policy, as determined by the Chief Privacy Official, must be included in contracts and other legally binding documents to ensure enterprise-wide compliance.

3. BACKGROUND

3.1 In order to comply with the Maryland Department of Information Technology (DoIT), IT Security Manual v. 1.2, (2019), MSDE is required to establish a Privacy Program consistent with NIST Special Publication 800-53 requirements.

3.2 This Policy forms a core component of the MSDE Privacy Program.

3.3 This Policy meets the requirements of the IT Security Manual v. 1.2, (2019) and provides additional safeguards consistent with Data Governance standards established by National Institute of Standards and Technology (NIST), the Centers for Medicare and Medicaid Services (CMS), Internal Revenue Service (IRS), Office of Legislative Audits (OLA), Office of Management and Budget (OMB), and the General Services Administration (GSA) as well as the requirements of the Family Educational Rights Privacy Act (FERPA).

4. SCOPE

4.1 MSDE collects PII for use in its mission to develop and implement standards, policies, and guidance for education programs from pre-kindergarten through high school.

4.2 PII may be collected, captured, and used in structured and unstructured format.

4.4 This Policy comports with the requirements of AR-7 Privacy Enhanced System Design and Development found in the IT Security Manual v. 1.2, (2019) at https://doit.maryland.gov/Documents/Maryland%20IT%20Security%20Manual%20v1.2.pdf

4.4 This Policy applies to all personnel, including contractors, partners and vendors, and to all data collection and use activities carried out by MSDE business units.

4.4 This policy is related to other MSDE policies and procedures, including:

- AD 21201-002 Access Control Policy
- AD 21201-003 Audit and Accountability Policy
- AD 21201-004 Identification and Authentication Policy

5. POLICY

MSDE has implemented a privacy risk management process that assesses privacy risk to individuals resulting from the collection, use, storage, transmission, and disposal of PII.

5.1 Authority and Purpose

The following controls ensure identification of the legal basis that authorizes collection of PII or any activity which may impact privacy. Furthermore, this control family outlines the purpose(s) for which the data is being collected.

5.1.1 MSDE determines and documents its legal authority to collect, use, maintain, and share PII, either generally or in support of a specific program or information system requirement.

5.1.2 MSDE describes in its privacy notices the purpose(s) for which PII is collected, used, maintained, and shared.

5.2 Accountability, Audit and Risk Management

The privacy controls below provide an overview of the governance, monitoring, risk management, and assessment used within MSDE.

5.2.1 MSDE must establish a Privacy Program consistent with NIST and IT Security Manual v. 1.2, (2019) requirements.

5.2.2 All data users and data owners, including business partners (vendors and service providers) are to be held accountable for compliance with this Policy and with the principles evoked in the IT Security Manual v. 1.2, (2019).

5.2.3 MSDE must document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, storage, sharing, transmitting, use, and disposal of PII.

5.2.4 MSDE must conduct Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs) for information systems, programs, and other activities that potentially pose a risk to the privacy and handling of PII.

5.2.5 MSDE must establish privacy roles, responsibilities, and access requirements for contractors and service providers.

5.2.6 MSDE must include privacy requirements in contracts and other acquisition-related documents.

5.2.7 MSDE must develop, implement, and update a comprehensive privacy training and privacy awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures.

5.2.8 MSDE must administer basic privacy training at least annually, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least annually.

5.2.9 MSDE must design information systems that support privacy with automated privacy controls.

5.2.10 MSDE must keep an accurate accounting of disclosures of information held in each system of records under its control, including:

- Date, nature, and purpose of each disclosure of a record; and
- name and address of the person or agency to which the disclosure was made.

5.2.11 MSDE must retain accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer, and must make the accounting of disclosures available to the person named in the record upon request.

5.3 Data Quality and Integrity

These controls ensure that PII which is collected and maintained is accurate, relevant, timely, and complete for the purpose for which it is to be used.

5.3.1 MSDE confirms, to the greatest extent practicable, upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.

5.3.2 MSDE collects PII directly from the individual or the individual's authorized representatives to the greatest extent practicable.

5.3.3 MSDE checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems.

5.3.4 MSDE issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

5.3.5 MSDE requests the individual or the individual's authorized representative to validate PII during the collection process.

5.3.6 MSDE documents processes and procedures to ensure the integrity of PII through existing security controls.

5.4 Data Minimization

Data minimization and retention controls assist MSDE to collect, use, and retain only relevant PII necessary for the original purpose for which it is collected.

5.4.1 MSDE must identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.

5.4.2 MSDE must limit the collection and retention of PII to the minimum elements identified, for the purposes described in the notice, and for which the individual has provided consent.

5.4.3 MSDE must conduct an initial evaluation of PII holdings. Afterwards, the Agency must periodically review the holdings annually. During the review the Agency must ensure that only PII identified in the privacy notice is collected, retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

5.4.4 MSDE must, where feasible and within the limits of technology, locate and remove/redact unnecessary PII. The Agency may use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

5.4.5 MSDE must retain each collection of PII for the minimum necessary time period to fulfill the purpose(s) identified in the notice or as required by law.

5.4.6 MSDE must dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule. This must be conducted in a manner that prevents loss, theft, misuse, or unauthorized access.

5.4.7 MSDE must use legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

5.4.8 MSDE must develop policies, procedures, and techniques to implement controls that minimize the use of PII for testing, training, and research.

5.5 Individual Participation and Redress (IP)

These requirements address the establishment of policy and procedures for the effective implementation of the controls and control enhancements of IP.

5.5.1 MSDE must provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

5.5.2 MSDE must provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII.

5.5.3 MSDE must obtain consent, where feasible and appropriate, from individuals before any new uses or disclosures of previously disclosed PII.

5.5.4 MSDE must ensure individuals are aware of and, where feasible, consent to specific uses of PII not initially described in the public notice.

5.5.5 MSDE must implement mechanisms, where possible, to support itemized or tiered consent for

specific uses of data.

5.5.6 MSDE must provide individuals with the ability to request and review their PII maintained in its system(s) of records.

5.5.7 MSDE must publish policies, procedures, and/or regulations governing how individuals may request access to records maintained in the system of records.

5.5.8 MSDE must provide information to individuals concerning how to correct or amend, as appropriate, inaccurate PII. This should include contact information for the entity that maintains the PII.

5.5.9 MSDE must establish a process for disseminating corrections or amendments of PII. The process shall include corrections within MSDE or other authorized users, such as external information sharing partners. Where feasible and appropriate, MSDE shall notify affected individuals when their information has been amended.

5.5.10 MSDE must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

5.5.11 MSDE must respond to complaints, concerns, and questions from individuals within a 72-hour time period.

5.6 Security

This section identifies the security controls to ensure technical, physical, and administrative safeguards are in place to protect PII collected or maintained by MSDE.

5.6.1 MSDE must establish, maintain, and update inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing PII every 365 days. The Agency shall provide each update of the PII inventory to the MSDE Chief Privacy Officer or Chief Information Security Officer.

5.6.2 MSDE must implement a Privacy Incident Response Plan.

5.6.3 MSDE must provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

5.6.4 MSDE must follow current Maryland Law requirements for providing notice to affected parties and reporting incidents to the required organizations, including the Maryland Department of Information Technology (DoIT) and the Maryland Attorney General (AG), as defined in MD State Gov Code § 10-1305 (2017).

5.7 Transparency

MSDE provides public notice of their information practices and the privacy impact of their programs and activities.

5.7.1 MSDE must

a. Provide effective notice to the public and to individuals regarding:
   1. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
   2. authority for collecting PII;
   3. the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
   4. the ability to access and have PII amended or corrected if necessary.

b. Describe:
   1. PII the organization collects and purpose(s) for which it collects the information;
   2. how the organization uses PII internally;
   3. whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
   4. whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
   5. how individuals may obtain access to PII; and
   6. how the PII will be protected.

c. Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable after the change.

5.7.2 MSDE must provide real-time and/or layered notice to individuals at the time when any PII is collected.

5.7.3 MSDE must ensure the public has access to information about its privacy activities and is able to communicate with its designated privacy official.

5.7.4 MSDE must ensure its privacy practices are publicly available through organizational websites or otherwise.

5.8 Use Limitation

MSDE will only use PII either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law.

5.8.1 MSDE must use PII internally only for the authorized purpose(s) identified in public notices.

5.8.2 MSDE must share PII externally, only for the authorized purposes identified and/or described in its notice(s) or for a purpose that is compatible with those purposes.

5.8.3 When sharing PII, MSDE must enter into appropriate agreements with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.

5.8.4 MSDE must monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

5.8.5 MSDE must evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

6. ROLES AND RESPONSIBILITIES

6.1 The Chief Privacy Officer (CPO) must determine how best to incorporate effective privacy protections and practices (e.g., privacy controls) within MSDE programs and information systems and the environments in which they operate.

6.2 In addition, as required by Maryland Executive Order 01.01.2021.10, the CPO will meet at least monthly to provide the State Chief Privacy Officer with advice and recommendations about State policies to protect the privacy of PII.

6.3 The CPO shall work in conjunction with others in MSDE to establish and maintain a cohesive and complete privacy program.

6.4 The CPO shall manage risk related to information privacy laws and compliance regulations.

6.5 The CPO shall utilize the privacy controls listed in the IT Security Manual v. 1.2, (2019) and NIST guidelines to work with program managers, mission/business owners, information owners, CIO, CISO, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (e.g., privacy controls). This is to be conducted within MSDE programs, information systems, and the environments in which they operate.

6.6 The Information System Owner (also referred to as System Owner or "SO") is responsible for the procurement, development, integration, modification, operation, maintenance, and retirement of an information system.

6.7 The SO has development and operational responsibility for the information system (IS) . Multiple SOs can be designated as required, however each IS must have atleast one (1) assigned SO.

6.8 The SO has the responsibilities enumerated in the IT Security Manual v. 1.2, (2019) including categorizing all information systems according to information type collected, maintained, used, stored, or processed by or on behalf of each agency. This is based on the objective of providing appropriate levels of information security according to a range of risk levels and in accordance with the Federal Information Processing Standard (FIPS) Publication 199.

6.9 The SO will work with the CPO to perform risk assessments (RA) annually or as part of continuous monitoring activities, to re-evaluate sensitivity of the system, risks, and mitigation strategies.

6.10 All personnel, contractors, vendors and service partners have roles and responsibilities to comply with this Policy and any other related policies to ensure a compliant environment.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

7.1 A violation of any of the responsibilities and conduct standards contained in this Policy may be cause for disciplinary or adverse action.

7.2 Disciplinary or adverse action will be applied in accordance with applicable law and regulations.

7.3 Personnel or organizations who commit policy infractions, intentional or unintentional, including misuse of MSDE IT resources, may be subject to disciplinary actions.

7.4 These disciplinary actions may include removal. Contractor employees may have their access privileges revoked and the contract could be terminated as a result of an infraction.

7.5 In addition to disciplinary action, system access privileges may be revoked.

7.6 When such actions appear to be criminal in nature, the matter must be referred to the DoIT Service Desk at Service.Desk@maryland.gov, and an incident response ticket will be created.

8. POLICY EXCEPTIONS

8.1 All divisions are required to conform to this policy. If a policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the user or system into compliance with policy but may serve as an indication of intent.

8.2 Policy waiver request memorandum will be addressed to the MSDE CIO and submitted to ato.msde@maryland.gov for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

9. UPDATES

9.1 Updates and new policies will be posted on https://oit.msde.maryland.gov.

9.2 This policy will be reviewed and updated at least every three years and the procedures reviewed and updated at least annually.

APPENDIX A - DEFINITIONS

Chief Information Officer (CIO): A chief information officer is the company executive responsible for the management, implementation, and usability of information and computer technologies.

Chief Information Security Officer (CISO): A chief information security officer is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Chief Privacy Officer (CPO): The Chief Privacy Officer is the executive responsible for the protection, preservation and principles of PII.

Information System Security Officer (ISSO): The Information System Security Officer serves as the principal advisor to the Information System Owner (SO), Business Process Owner, and the CISO on all matters, technical and otherwise, involving the security of an information system.

Personally Identifiable Information (PII): The term "PII," as defined in State Government Art. 10-1301 as "an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combinationwith one or more of the following data elements:

1) Social Security number;
2) driver's license number, state identification card number, or other individualidentification number issued by a unit;
3) passport number or other identification number issued by the United States government;
4) Individual Taxpayer Identification Number (ITIN); or financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code,or password, would permit access to an individual's account.

Personnel: Employees and contractual employees of MSDE.

Sensitive Information: Information that, if divulged, could compromise orendanger the citizens or assets of the State. Types of sensitive information may include human resource information, including personal files, educational, and financial records, personal health information, procurement sensitive information, information protected by Nondisclosure Agreement (Example, State proprietary information), business proprietary information given to MSDE as part of contracts or agreements, other information identified by the information owner and Agency policy or programs as sensitive.

System Owner (SO): The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The SO could be a Program Manager, an Application Manager, an IT Director, or an Engineering Director.

APPENDIX B - ACRONYMS AND ABBREVIATIONS

AD	Agency Directive
AP	Authority and Purpose
AR	Accountability, Auditing and Risk Management
AUP	Acceptable Use Policy
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CPO	Chief Privacy Officer
DI	Data Quality and Integrity
DM	Data Minimization
DoIT	Department of Information Technology
FERPA	Family Educational Rights and Privacy Act
FISMA	Federal Information System Management Act
GSA	General Services Administration
IP	Individual Participation and Redress
IT	Information Technology
MSDE	Maryland State Department of Education
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OLA	Office of Legislative Audits
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SE	Security
SO	System Owner

APPENDIX C - AUTHORITY AND REFERENCES

Executive Order 01.01.2021.10, Maryland Data Privacy,

https://governor.maryland.gov/wp-content/uploads/2021/07/Maryand-Data-Privacy-EO.pdf

Family Educational Rights and Privacy Act (FERPA), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Maryland Department of Education (MSDE), AD 21201-001, *Security Awareness and Training Policy*, March 2021

Maryland Department of Information Technology (DoIT), IT Security Manual, *Information Technology Security Manual*, Version 1.2, June 2019

National Institute of Standards and Technology (NIST) Special Publication (SP), NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003

National Institute of Standards and Technology (NIST) Special Publication (SP), NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2021

National Institute of Standards and Technology (NIST) Special Publication (SP), FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

National Institute of Standards and Technology (NIST) Special Publication (SP), FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

National Institute of Standards and Technology (NIST) Special Publication (SP), NISTIR 7316, *Assessment of Access Control Systems*, September 2006

OMB, M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

APPENDIX D - NOTICE OF POLICY CHANGES

Privacy Policy Changes

Changes to our websites may necessitate changes to our privacy statement. Notification will be posted on the Maryland State Department of Education website homepage at www.marylandpublicschools.org in the Privacy link. The information contained in this website privacy statement applies only to www.marylandpublicschools.org and other State agency websites that have been authorized to link to this policy, and not to any linked sites or all websites maintained by Maryland State agencies. You should review the individual privacy statements at any linked site that you visit.

Signature: Mohammed Choudhury
Mohammed Choudhury (Jan 27, 2023 16:03 EST)

Email: Mohammed.Choudhury@maryland.gov