STATE OF NEW JERSEY
DEPARTMENT OF EDUCATION

Data Security & Privacy Policy - April 2020

Overview

The New Jersey Department of Education (NJDOE or Department) is required by law to collect and store student and educator records and takes seriously its obligation to secure information systems and protect the privacy of student data that is collected, used, shared and stored by the Department. In addition to the laws that require the NJDOE to collect educational data, these data assets are essential to the NJDOE's strategic operations and support of local educational entities, and they must be diligently protected.

As a standard operating procedure, the NJDOE regularly monitors changes in state and federal regulations that are related to data collection, privacy and security. The NJDOE meets all state and federal requirements related to data security and IT infrastructure, as well as the policies and processes encompassed within this data privacy and security policy.

Data Privacy

Internal Use of Data

The students' and educators' records that the NJDOE collects and stores from LEAs and schools are used for compliance, audit and evaluation purposes. This information is only available to employees and contract partners who have a responsibility and appropriate need for accessing the information. The NJDOE's Data Management Office is responsible for developing and implementing the policies and procedures that assure data is properly handled throughout the data lifecycle. As part of these processes, the Data Management Office tracks the list of the specific individuals within the Department who have access to student and educator data systems, as well as the specific data that are being requested.

External Use & Disclosure of Data

The NJDOE may release both identified and de-identified data through a formal Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) process, also known as Data Sharing Agreements. All Data Sharing Agreements must contain specific terms and conditions related to confidentiality, data privacy and security, record-keeping and data ownership. Each written agreement must clearly outline strict requirements that a research institution or institution of higher learning must agree to in order to receive data. In addition, all research requests are vetted through the research institution's Institutional Review Board (IRB) as part of their MOU/MOA process. The IRB must review and approve or reject all requests to conduct research using any student or school system data requested from the NJDOE prior to submission. The contracting agency is responsible for ensuring that any research or analysis shared is "de-identified" so that individual students are not personally identifiable. Those

requesting any data from the NJDOE must meet all criteria outlined in the MOU/MOA processes prior to obtaining data access.

The NJDOE has the right to reject any research proposal submitted.

When providing or delivering data to any stakeholder using any delivery mechanism, the Department maintains compliance with the Family Educational Rights and Privacy Act (FERPA), 34 CFR § 99.31. For more information on FERPA, please visit the United States Department of Education's Family Educational Rights and Privacy Act (FERPA) page.

If an individual is concerned about an alleged violation of a Data Sharing Agreement, a written complaint should be submitted to the NJDOE, including the specific allegations of fact(s) giving reasonable cause to believe that a violation occurred. The NJDOE will investigate all reasonable and timely complaints. The NJDOE may also conduct investigations without the filing of a formal complaint to determine whether a violation has occurred.

When contracting with vendors, the NJDOE follows all federal and state statutory and regulatory requirements to protect its data and data systems. Vendors must first pass a System Architecture Review, completed by NJOIT (New Jersey's Office of Information Technology). The review outlines the security infrastructure and database architecture to be used, detailing the encryption processes for storing Personally Identifiable Information (PII) or confidential data. All PII must be protected and classified in accordance with the state's Asset Clarification and

Control Policy (08-04-NJOIT), and then disposed of in accordance with the state's Information Disposal and Media Sanitation Policy (09-10-NJOIT).

Sensitive data transmission is only permitted using the secure file transfer methodologies that meet the state and federal security guidelines and the standards outlined by NJOIT. The state may revise or change the file transfer methodology at any time, and contractors are required to conform to secure file transfer requirements. Data storage and protection are also subject to all state and federal requirements, including encryption for all data defined as confidential or PII, and contractors are required to conform to Payment Card Industry (PCI) Data Security Standards. When contracts with vendors expire or are terminated, the contractor is required to first return all data to the state, then erase, destroy or render unreadable all contractor copies of state data, in accordance with the Information Disposal and Media Sanitation Policy.

Certification in writing of the completion of that process must occur within 30 days of the contract end-date.

Breaches in Security

Concerns about security breaches must be reported immediately to the NJDOE's Chief Information Technology Officer. If the Chief Information Technology Officer, in collaboration with the Commissioner and other appropriate members of the executive team, determines that an

employee(s) and/or contracted party have failed to comply with the NJDOE's or state of New Jersey's Online Privacy Policy, they will identify appropriate consequences to be applied. These can be as severe as termination of employment or contract and/or further legal action.

Concerns about a breach involving the NJDOE's Information Technology Office should be reported immediately to the Commissioner using the Parent Contact Form.

If there is a data breach with a vendor/contractor, the contractor must comply with all applicable state and federal laws that require the notification of individuals in the event of unauthorized release of PII. Contractors must notify the NJDOE within 24 hours of the incident. The NJDOE reserves all rights to act under the terms of the contract or memorandum of understanding, including indemnification and/or termination of the contract.

Data Governance

The NJDOE is committed to protecting and safeguarding the data that it collects and recognizes data as a critical asset. A three-tiered governance structure, managed by the Office of Data Management, controls the organization's approach to data and information management through an agency-wide infrastructure that ensures appropriate data use, management of change and support for the implementation of security and privacy protocols. This agency-wide infrastructure is the mechanism for ensuring appropriate data use, managing change and supporting the implementation of security and privacy protocols.

Staff Training

In order to maintain the highest data security and quality standards, optimize data use and minimize misuse of information, the NJDOE provides training opportunities for all staff who use educational data. Additionally, all new NJDOE employees must sign and obey the NJDOE Acceptable Use of Information Technology Resources Policy, which describes the permissible uses of state technology and information.

Additional Resources

FERPA

- Family Educational Rights and Privacy Act (FERPA)
- FERPA General Guidance for Parents

SPPO

Student Privacy Policy Office (formerly the Family Policy Compliance Office or FPCO and the Privacy Technical Assistance Center or PTAC).

- Policies for Users of Student Data: A Checklist
- Protecting Student Privacy While Using Online Educational Services
- Early Childhood Data Privacy