

Sounding Board

A publication of Osprey Wilds Environmental Learning Center Charter School Division



The Minnesota Government Data Practices Act

October 2023

Introduction

As a governmental entity, charter schools are subject to the rights and obligations of the Minnesota Government Data Practices Act (the “MGDPA”). This article seeks to give a basic foundation and understanding of the MGDPA and its applicability to charter schools. Nonetheless, given the complexity of the MGDPA, and the potential for litigation and civil penalties for violations of the MGDPA, charter schools should do additional diligence to familiarize themselves with the provisions of the MGDPA, as well as contemplate hiring legal assistance to help develop policies and procedures to comply with the MGDPA.

What is the MGDPA?

Generally speaking, the MGDPA is a Minnesota law that governs how governmental entities such as charter schools can collect, create, store, use, and release data. The MGDPA establishes a system of data classifications that define, in general terms, who is legally authorized to access government data. The MGDPA specifies that all government data is public unless a statute, rule, or a federal law classifies the data as, with respect to data on individuals, private or confidential; or, in the case of data not on individuals, as nonpublic or protected nonpublic.

“Data on individuals” is all government data in which any individual is or can be identified as the subject of that data. Data on individuals are classified as public, private, or confidential. In contrast, “Data not on individuals” is all government data which is not data on individuals, and are classified as public, nonpublic, or protected nonpublic. This classification system determines how government data are handled.

- **Public data:** Public data is accessible by anyone. The MGDPA provides that, unless specifically authorized by statute, a government entity may not require persons to identify themselves, state a reason for, or justify a request to gain access to public government data.
- **Private data:** Private data on individuals is data classified by statute or federal law as not public but accessible to the individual subject of that data.
- **Confidential data:** Confidential data on individuals is data made not public by statute or federal law and is inaccessible to the subject of that data.
- **Nonpublic data:** Nonpublic data is data not on individuals that a statute or federal law makes not accessible to the public but accessible to any subject of that data.
- **Protected nonpublic data:** Protected nonpublic data is data not on individuals which is both not public and not accessible to the subject of that data.

The most important type of data that charter schools will be concerned about, is the collection, creation, storage, use, and release of “Educational Data,” which is considered private data and may only be released in certain circumstances.

What is Educational Data?

Educational Data is defined as “data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student.”

Below is a list of some important caveats and contours surrounding Educational Data:

- Teacher’s personal records
 - Educational Data does not include personal records of a teacher that are not accessible or revealed to any other individual (must be destroyed at the end of the year, and can be released to a substitute teacher).
- Health Data
 - Educational Data includes the health data of students such as immunizations, notations of special physical or mental problems, records of school nurses, and emergency contact and family information.
- Directory Information
 - Directory information of a school is public information that can be freely collected, used, and released, but the school must give the parents and students notice of the right to refuse the designation of any or all data about the student as “directory information.” Directory information generally includes: the student’s name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.
- Parent Data
 - Data concerning parents are generally private data, but may be treated as directory information if the parents are given notice of the right to refuse the data from being designated as directory information.

What must a school do before collecting private data?

Before collecting information that is deemed to be private information by virtue of a federal or state law, on a student, parent, or employee, a school must inform the individual of:

- the purpose and intended use of the requested data within the collecting government entity;
- whether the individual may refuse or is legally required to supply the requested data;
- any known consequence arising from supplying or refusing to supply private or confidential data; and
- the identity of other persons or entities authorized by state or federal law to receive the data.

This is commonly referred to as the “Tennessee warning,” and failure to give such warning prevents a school from being able to use, collect, store, or release the data.

When can Educational Data be released?

Under the MGDPA, Educational Data is private data and shall not be disseminated without the subject of the data first giving informed consent, unless specific exceptions under the MGDPA exist. Below is a non-exhaustive list of the most common exceptions where a school is authorized to disclose Educational Data:

- Valid Court Order
 - It is being disclosed pursuant to a valid court order.
- Statute
 - It is being disclosed pursuant to a statute specifically authorizing access to the private data.
- Emergency
 - It is being disclosed in connection with a health (including mental health) or safety emergency.
- School Official with Legitimate Educational Interest
 - It is being disclosed to other school officials who have legitimate educational interest, including the educational interest of the child.
- School Official of Another School with Legitimate Educational Interest
 - It is being disclosed to school officials of another school in which the student seeks to enroll, as long as parent receives a copy of the record if desired (parent can also challenge content of record).
- Educational Studies
 - It is being disclosed in connection with organizations conducting studies for educational agencies for the purpose of developing, validating, or administering predictive tests or improving instructions, as long as such studies are conducted to not permit personal identification of students and their parents by persons other than the representatives of such organizations.
- Educational Volunteers with Legitimate Educational Interest
 - It is being disclosed to volunteers who are determined to have a legitimate educational interest in the data and who are conducting activities and events sponsored by or endorsed by the educational agency or institution for students or former students.
- Reporting Behavior to Juvenile Justice System
 - It is being disclosed to the juvenile justice system if information about the behavior of a student who poses a risk of harm is reasonably necessary to protect the health or safety of the student or other individuals.
- Reporting Maltreatment of a Student
 - It is being disclosed to the commissioner of education for purposes of an assessment or investigation of a report of alleged maltreatment of a student.



- Request by the Juvenile Justice System
 - It is being disclosed to the appropriate authorities of the juvenile justice system, provided that the authorities certify in writing that the data will not be disclosed to any other person without the written consent of the parent, and a record of such consent will be maintained in the student's file. The following information must be disclosed pursuant to this exception includes: a student's full name, home address, telephone number, date of birth; a student's school schedule, daily attendance record, and photographs, if any; and parents' names, home addresses, and telephone numbers. Moreover, a simple yes or no response (cannot provide the actual data) with regard to the following information may be disclosed pursuant to this exception: drug use, assaultive or threatening behavior, possession or use of weapons, theft, or vandalism. However, this second category of information cannot be released unless the school notifies the student's parent or guardian of the request, and the parent or guardian does not object to the disclosure within 10 days of receipt. If the parent or guardian does object within the time frame, then the school must inform the requesting member of the juvenile justice system of the objection. A school must respond to a juvenile system's request for information within 14 days if no objection from the parent or guardian is received. There is a specific form set forth in Minnesota Statute § 13.32 that the juvenile system is required to use to request that second category of information, and schools should request compliance with that form in the event a school receives a request not in compliance with that form.
- Request by an Adult Individual Granted Access Rights
 - It is being disclosed to an adult individual that has been granted access to a student's records by virtue of the parent or guardian of that student provided prior written notice of consent to the school. The consenting guardian or parent can revoke their consent at any time.
- Request by a Parent of a Child
 - It is being disclosed to a parent or guardian of a child. A school cannot charge a fee for providing the information, but may charge a fee for copies.
- Request by the Welfare System
 - It is being disclosed to the county personnel in the welfare system in order to coordinate services for a student or family. A request by a county personnel must include the basis for the request and a description of the information that is requested. The school then must provide a copy of the request to the parent or legal guardian of the student who is the subject of the request, along with a form the parent or legal guardian may execute to consent to the release of specified information to the requester. If the parent does not consent, then the information may not be released to the county personnel.
- Request by Military Recruitment Office
 - A school must release the names, addresses, and home telephone numbers of students in grades 11 and 12 within 60 days of a request from a military recruiting office. However, the school must give parents and students notice of the right to refuse the release of such information.
- For the Safety of School Employees
 - Schools that receive copy of a disposition order from a juvenile court are authorized to collect that information as part of the student's education record, and must notify any counselor or teacher, or other employee in order to avoid someone being needlessly vulnerable. It is still otherwise private data and should not be disseminated to anyone other than those employees that serve the student, in order to protect themselves.

Can a student request their own Educational Data?

An individual student who is the subject of stored private data has the right to be shown the data free of cost (if an individual requests copies, a school can charge the actual cost for those), and has the right to be informed of the content and meaning of that data. An individual does not have a right to see their private data more than once every six months, unless a dispute arises. The designated data representative for the school shall provide the information immediately upon request.

If for some reason the information is not available immediately, the information shall be provided no later than 10 weekdays after the request, excluding holidays. This deadline also applies to any request to a school by individuals (students, employees, parents), seeking public or private information about themselves held by that school. An individual student does have the authority to contest the accuracy or completeness of the data in the manner set forth in the statute. However, it is important to note that a student does not have the right to access the financial records and statements of the student's parents.



What data safeguards must be in place with regard to services provided to a charter school by a technology provider?

A contract between a technology provider and a school must state that the technology provider's employees only have access to educational data if authorized, and the employees may be authorized to access educational data only if access is needed to fulfill the official duties of the employee. Moreover, within 30 days of the start of each school year, a charter school must give parents and students direct and timely notice of:

- each curriculum, testing, or assessment technology provider with access to educational data;
- the educational data affected by the curriculum, testing, or assessment technology provider contract; and
- information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.

A charter school must also give parents and students an opportunity to inspect a complete copy of any contract with a technology provider.

What restrictions must be in place with regard to school-issued devices?

Subject to the exceptions listed below, a charter school (or technology provider) may not electronically access or monitor:

- any location-tracking feature of a school-issued device;
- any audio or visual receiving, transmitting, or recording feature of a school-issued device; or
- student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

The exceptions to the prohibitions above are:

- the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by district employees, student teachers, staff contracted by a district, a vendor, or the Department of Education, and notice is provided in advance;
- the activity is permitted under a judicial warrant;
- the public educational agency or institution is notified or becomes aware that the device is missing or stolen;
- the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose (however, must notify student or student's parent within 72 hours of the access (description of access and what features were accessed) under this exception, unless the notice itself would be a danger to the student, then within 72 hours after the threat to life or safety has ceased).
- the activity is necessary to comply with federal or state law
- the activity is necessary to participate in federal or state funding programs

What happens if there is a breach of Educational Data?

In the event that there is a breach of educational data collected and stored by a charter school, the school must give written notice to any individual whose data was private and was (or reasonably believed to have been) released to an unauthorized person. The notice must also state that a report will be prepared and that the individual has the ability to access the report. This notice should be made as soon as possible, but consistent with the legitimate needs of a law enforcement agency.



Upon completion of an investigation into any breach, a report shall be prepared reporting on the facts and results of the investigation. If the breach involves the unauthorized access of data regarding an employee, contractor, or agent of the school, then the report must include (i) a description of the type of data that was acquired, (2) the number of individuals affected, and (3) whether there has been a final disposition of disciplinary action (including the names of any employee determined to be responsible for the unauthorized access (subject to some exceptions).

Additional Educational Data rules outside of the MGDPA

In addition to the information provided in the sections above, charter schools should be versed in the following additional statutes that implicate the use, collection, and release of Educational Data.

Namely:

- Testing Data
 - Data sharing involving the statewide testing and reporting system is governed by sections 120B.30, subdivision 3, and 120B.31, subdivision 4.
- School Accountability
 - School accountability data is governed by sections 120B.35, subdivision 3, and 120B.36, subdivisions 1, paragraph (e), and 2.

- Disposition Orders Received by Schools
 - Access to disposition orders received by schools is governed by section 121A.75.
- Students Rights, Responsibilities, and Behavior
 - Data sharing involving immunization records is governed by section 121A.15, subdivision 7.
 - Data collected in early childhood developmental screening programs are classified under section 121A.18.
 - Data sharing involving exclusions and expulsions is classified under section 121A.53.
- Teachers Discharges and Resignations
 - Data on certain teacher discharges and resignations reported under section 122A.20 are classified under that section.
- Energy Efficiency Projects
 - Data involving energy efficiency project contracts are governed by section 123B.65, subdivision 10.
- Performance Tracking Systems:
 - Data sharing related to the performance tracking system is governed by section 124D.52.
- Special Education
 - Disclosure of special education student data to health plan companies is governed by section 125A.21, subdivision 7.
 - Agency access to data about a child with a disability is governed by section 125A.23.
 - Data sharing involving interagency early intervention committees is governed by sections 125A.027, subdivision 1, and 125A.30.
- Military-connected Youth Identifier
 - Data collected on enrollment forms to allow students to self-identify as military-connected youth are governed by section 127A.852.
- High School League
 - Data involving the High School League are governed by section 128C.17.
- Teacher Data from Value-Added Assessment Model
 - Data on individual teachers generated from a value-added assessment model are governed under section 120B.35.
- Student Progress
 - Data practices governing the world's best workforce under section 120B.11 and student progress data under section 120B.35 are governed by section 120B.36, subdivision 2.

What employee records are public?

With regard to data on current and former employees, volunteers, and independent contractors of a charter school, the following information is public:

- name; employee identification number, which must not be the employee's Social Security number; actual gross salary; salary range; terms and conditions of employment relationship; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary;
- job title and bargaining unit; job description; education and training background; and previous work experience;

- date of first and last employment;
- the existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action;
- the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body;
- the complete terms of any agreement settling any dispute arising out of an employment (subject to some restrictions)
- work location; a work telephone number; badge number; work-related continuing education; and honors and awards received; and
- payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data.

What are the consequences for failing to comply with the provisions of the MGDPA?

A charter school may be sued to compel compliance with the MGDPA, and forced to pay a civil penalty up to \$1,000, and pay the aggrieved person's costs and attorney's fees. There are more severe consequences for willful violations of the MGDPA.

Conclusion

As a custodian of private data, charter schools must be aware of their obligations to maintain the privacy of data on individuals, as well as their duty to disclose public data when requested. Schools can prepare by having data privacy policies in place, and by designating an individual to whom to direct all data requests so that requests for data can be handled promptly within statutory deadlines.

