Ratwik, Roszak & Maloney, P.A.

444 Cedar Street, Suite 2100
Saint Paul, Minnesota 55101

(612) 339-0060
www.ratwiklaw.com

WHO NEEDS TO KNOW?
DATA PRIVACY AND SPECIAL EDUCATION

Christian R. Shafer
crs@ratwiklaw.com

Adam J. Frudden
ajf@ratwiklaw.com

MASE FALL LEADERSHIP CONFERENCE
October 24, 2025

From e-mails to PWNs, all information created, collected, maintained, or disclosed by a school about a student with a disability is subject to a variety of laws. In this presentation, experienced school attorneys will discuss the applicable statutory schemes and provide practical, real-world solutions to some of the most common questions about access to, and protection of, special education records.

I. LAWS GOVERNING DATA PRIVACY.

A. The Family Educational Rights and Privacy Act ("FERPA")

FERPA is a federal law that protects the privacy of student education records. FERPA applies to educational agencies and institutions that receive funds under

any program administered by the U.S. Department of Education ("U.S. DOE"). This includes virtually all public schools.

B. The Minnesota Government Data Practices Act ("MGDPA").

The MGDPA is a state law that controls how government data are collected, created, stored, maintained, used, released, and disseminated. The MGDPA sets out certain requirements relating to the right of the public to access government data and the rights of individuals who are the subjects of government data. Educational data is classified and governed by this law.

C. The Individuals with Disabilities Education Act ("IDEA").

The IDEA is a federal law that ensures students with a disability are provided with a free appropriate public education ("FAPE"). Pursuant to the IDEA, the United States Secretary of Education is required "to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State educational agencies and local educational agencies…." 20 U.S.C. § 1417(c).

II. GOVERNMENT DATA.

A. Government Data under the MGDPA.

1. Government data.

a. "Government data" is defined as all data collected, created, received, maintained, or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media, or conditions of use. Minn. Stat. § 13.02.

b. In order to be data under the MGDPA, the information must be recorded in some form. Unrecorded mental impressions of public employees are not government data. *Keezer v. Spickard*, 493 N.W.2d 614 (Minn. App. 1992). However, once data are recorded in any form, the data become "government data" regardless of their physical form, storage media, or the conditions of their use. Minn. Stat. § 13.02, subd. 7; *see also* Minn. R. 1205.0200, subp. 4.

c. Desk drawer records. "Records of instructional personnel which are in the sole possession of the maker thereof and are not accessible or revealed to any other individual except a substitute

teacher, and are destroyed at the end of the school year, shall not be deemed to be government data." Minn. Stat. § 13.32, subd. 1(a).

d. Nothing in the MGDPA requires government entities to create data on behalf of a parent, community member, or other person requesting data.

2. ***Data on Individuals***. Data on individuals is all government data in which an individual is or can be identified as the subject of that data, unless the identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by identifying data of any individual. Minn. Stat. § 13.02, subd. 5

3. ***Public, Private, and Confidential Data on Individuals***. The three types of data on individuals that generally arise in the educational setting are public data, private data, and confidential data.

a. Public Data on Individuals. Data that the public may access because no state or federal law or regulation denies such access. *See* Minn. Stat. § 13.02, subd. 15.

b. Private Data on Individuals. Data that the public is denied access by statute or federal law, but which is accessible to the subject of the data. Minn. Stat. § 13.02, subd. 12.

c. Confidential Data on Individuals. Data that is made not public by statute or federal law and as to which the subject of the data is also denied access. *See* Minn. Stat. § 13.02, subd. 3; *see also* Minn. R. 1205.0200, subp. 3.

4. ***Educational Data***.

a. Definition. Educational data means "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." *See* Minn. Stat. § 13.32.

b. Typically Private. Most educational records constitute private data on an individual and may not be disclosed to the public.

i. Videos of Student Misconduct. Video footage of student misconduct likely constitutes an educational record for purposes of FERPA and the MGDPA. *See Echo Newspaper*

v. St. Louis Park Pub. Schools, 2018 WL 3826264 (Minn. App. Aug. 13, 2018) (school's security camera footage of students who had been in altercation was an "educational record" under the MGDPA).

ii. Special Education Records. School staff should not post anything on social media (or anywhere else) identifying specific students as receiving special education, including pictures and/or comments which identify the student as a special education student. *See* Dept. of Administration Advisory Op. 04-024 (school district did not comply with the MGDPA in publishing a photograph of a student in the school's yearbook on a page that identified the student as receiving special education services).

c. Permitted Disclosures. There are situations in which a school can or must disclose educational data.

5. Personnel Data.

a. Definition. "Personnel data" means "government data on individuals maintained because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with a government entity." Minn. Stat. § 13.43, subd. 1.

b. Private Personnel Data. Personnel data about a current or former employee are private unless a specific statutory exception applies. *Id.*, subd. 2(a).

c. Permitted Disclosures. There are situations in which a school can or must disclose personnel data.

III. LIABILITY FOR IMPROPER DISTRIBUTION OF GOVERNMENT DATA.

A. MGDPA Claim.

1. Under Section 13.08, subdivision 1, a responsible authority or government entity which violates the MGDPA is liable to a person who suffers any damages as a result of the violation. That liability may cover damages sustained, plus costs and reasonable attorneys' fees. *See Navarre v. South Washington County Schools,* 652 N.W.2d 9 (Minn. 2002). A "willful violation" can result in punitive damages from $1,000.00 to $15,000.00

for each violation. An individual may bring an action against the entity to compel compliance with the MGDPA and recover the cost of doing so.

2. Any person who willfully violates the MGDPA or whose conduct constitutes the knowing unauthorized acquisition of not public data is guilty of a criminal misdemeanor. A willful violation of the MGDPA by any public employee also constitutes just cause for suspension without pay or dismissal of the public employee. Minn. Stat. § 13.09.

3. The statute does not mandate an award of attorneys' fees. A district court has discretion. *Star Tribune v. City of St. Paul*, 660 N.W.2d 821 (Minn. Ct. App. 2003).

B. Common Law Claims. Minnesota recognizes a common law action for invasion of privacy. *See Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998). Publication of private facts is an invasion of privacy when one gives publicity to a matter concerning the private life of another if the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public. *Id.*

C. Disclosing Data with Multiple Data Classifications. The Minnesota Supreme Court held that public disclosure of the results of an employment investigation resulting in a psychiatrist's termination did not violate the MGDPA, despite that the data disclosed were "duplicative" of confidential data contained in a maltreatment investigation report. *Harlow v. State of Minnesota Department of Human Services,* 883 N.W.2d 561 (Minn. 2016). The Court "acknowledged that it may seem anomalous to have data classified as public for one purpose, and confidential for another purpose. But we see nothing in the text of the MGDPA that prohibits this outcome." *Id.* at 568.

III. CONSIDERATIONS SURROUNDING GENERATIVE ARTIFICIAL INTELLIGENCE ("AI") AND APPROPRIATELY SAFEGUARDING GOVERNMENT DATA.

A. Generative AI.

1. The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content. U.S. DEPT. OF COMMERCE: NAT'L INST. OF STANDARDS AND TECH, NIST SP 800-218A.

2. With the increase in AI, many employees, including school staff and school administrators, have begun to use publicly available generative AI tools, such as ChatGPT when, for example, creating lesson plans or developing IEP paperwork.

B. State and Federal Guidance.

1. ***Minnesota Department of Education's ("MDE") Guidance***. In July 2024, MDE issued guidance on AI titled *Artificial Intelligence in Education*. MDE's guiding principles on AI include:

   a. "Data privacy, security and content appropriateness should be primary considerations when adopting new technology."

   b. "Decision-makers need to understand how AI models work so they can anticipate limitations, problems, and risks. Leaders should create a culture of continual evaluation and innovation to be ready to respond to future technology innovations and disruptions."

2. ***U.S. DOE Guidance.*** On July 22, 2025, the U.S. DOE provided guidance on the integration of AI in school districts, as well as other entities. *Dear Colleague Letter*, 125 LRP 21297 (U.S. DOE 2025).

   a. The U.S. DOE expects school districts to "apply sound judgment and partner with researchers, educators, and communities to ensure the effective, safe, and ethical deployment of AI."

   b. The U.S. DOE set forth the following principles for "all AI-related educational initiatives," that included that AI systems "must comply with federal privacy laws," including FERPA.

C. Key Point.

1. ***Generative AI Products.*** Many generative AI products incorporate whatever an individual inputs into their models, which can expose the substance of the information to other users outside of the school, and/or third-party service providers, their partners, and their sub-contractors to train AI models. *See, e.g.*, *The Cubicle Culprits: Insider Risk Report, Q1*, CYBERHAVEN (2024), at 9; *Use Generative AI Services Safely*, UNIVERSITY OF OXFORD: OXFORD SECURE, at https://www.infosec.ox.ac.uk/use-generative-ai-services-such-as-chatgpt-safely; Jack M. Germain, *Surge in 'Shadow AI' Accounts Poses Fresh Risks to Corporate Data*, TechNewsWorld, July 25, 2024, at https://www.technewsworld.com/story/surge-in-shadow-ai-accounts-poses-fresh-risks-to-corporate-data-179299.html; *see also* Lance Eliot, *Generative AI ChatGPT Can Disturbingly Gobble Up Your Private and*

Confidential Data, Forewarns AI Ethics and AI Law, FORBES, Jan. 27, 2023.

2. ***Key Point.*** School employees should *never* enter data or otherwise submit data that is considered private under the MGDPA or FERPA into these AI models.

3. ***Lawsuits.*** The *New York Times* filed a copyright infringement lawsuit against Microsoft Corporation and OpenAI. In its assertion of copyright infringement claims, the New York Times submitted an exhibit with over 100 examples of ChatGPT essentially regurgitating original articles written by the New York Times. *Id.* Many similar lawsuits have also been filed. *See, e.g.*, *Daily News L.P. v. Microsoft Corp. et al.*, 1:24-cv-03285 (S.D.N.Y.); *see also A.T. v. Open AI, et al.*, 3:23-cv-04557 (N.D. Calif. 2023) (class action lawsuit claiming use of stolen personal information from hundreds of millions of internet users).

III. INDIVIDUALIZED EDUCATION PROGRAMS, BEHAVIOR INTERVENTION PLANS, AND SECTION 504 PLANS.

All staff and substitute teachers who are responsible for implementing the individualized education program ("IEP"), behavior intervention plan ("BIP"), and/or Section 504 plan must be provided all portions of the IEP, BIP, and/or Section 504 plan that they need to know to ensure the IEP, BIP, and/or Section 504 plan are fully implemented. *See Johnston County Pub. Schs. (NC)*, 120 LRP 11396 (OCR Oct. 17, 2019) (finding that some substitute teachers may not have been aware of one of the provisions in a student's Section 504 plan and expressing "concerns" those substitute teachers "may have denied the Student a FAPE by failing to implement the aforementioned provision of the Student's Section 504 Plan"); *see also* Minn. R. 1205.0400, subp. 2 ("Access to private data shall be available [to]: . . . individuals within the entity whose work assignments reasonably require access.").

IV. GENERAL PRACTICES FOR SAFEGAURDING EDUCATIONAL DATA.

A. Preventing Unintentional Disclosure of Private Education Data

1. Discussing Student Information Practice Points.

b. Legitimate Educational Interest. School district staff can discuss personally identifiable information from a student's education records without the written consent of the student's parent to other school staff, including teachers, if the school has determined that

each recipient of the information has *a legitimate educational interest* in such records.

i. Note. The Minnesota School Boards Association defines legitimate educational interest as "an interest directly related to classroom instruction, teaching, student achievement and progress, discipline of a student, student health and welfare, and the ability to respond to a request for education data." MSBA Policy 515 – Protection and Privacy of Pupil Records.

ii. Practice Point. As a best practice, school professionals who have a legitimate educational interest in sharing private student educational data should not discuss student information in community areas such as hallways, lounges, and parking lots in order to prevent the unauthorized disclosure of private student data. Furthermore, school staff should carefully weigh the risks of the communication methods they use. Overall, school staff should refrain from discussing personal student information in public areas and be aware of the security risks of the communication methods used when sharing private student data, such as in emails or text messages.

2. Electronic Communication Techniques Practice Points.

a. Assume the data may be read by the subject of the data or the public.

b. Determine who should be included in email messages; be careful with autofill.

c. Consider who should be included in replies and review who is in fact included. Be careful not to "reply all" when there may be private data in an earlier part of a chain.

d. Begin a new email when the subject changes when addressing private or confidential data. This minimizes the need to redact data. When replying to emails, the reply should be limited to that subject only.

e. Determine how to store the data if it needs to be retained, either electronically or in printed form.

f. Ensure that communications with legal counsel are protected.

g. Take care to physically protect data from improper disclosure through use of passwords and maintaining physical copies of data in a safe and secure manner.

i. Prohibit passwords that are obvious, such as nicknames, dates of birth, names of family members or pets, or hobbies.

ii. Prohibit the storage of passwords and other confidential, private, and not public data on mobile devices.

iii. Prohibit disclosure of employee PINs or passwords to anyone, with the exception for testing by IT staff to resolve a problem. Passwords should be changed after being shared with IT staff.

h. Report all lost or stolen devices with access to or containing private data.

i. Use discretion. As a general rule, school staff and school administrators should not put anything in writing that they would not want read out loud in court. It is possible that every social media post, email, text and/or instant message may become part of the record in administrative proceedings and/or litigation.

3. ***Employee Social Media Use Practice Points*.** School staff should not post private data on social media (or anywhere else). *See* Dept. of Administration Advisory Op. 04-024.

4. Proper Disposing of Student Information

a. *Scott v. Minneapolis Public Schools*, 2006 WL 997721 (Minn. Ct. App. 2006).

i. The Minnesota Court of Appeals found that the *inadvertent release of data* was not a defense to a claim for damages under the MGDPA where sensitive educational records arising out of the evaluation of a special education student were found, and circulated by other students, after the records blew out of a dumpster behind a school building.

ii. "Because the responsible authority…did not prescribe appropriate methods for destruction of student data, the jury had basis to find that the school district did not establish appropriate security safeguards and thus violated the Data Practices Act by failing to perform a duty set forth in Minn. Stat. § 13.05, subd. 5(2)." *Id.*

b. Practice Point. Consider ways to prevent inadvertent disclosures in today's high-tech world. What ways might school staff inadvertently disclose private educational or personnel data with today's technology? Be careful not to:

i. Inadvertently include improper recipients on an email, messaging application, or shared document that contains private data.

ii. Lose or improperly dispose of external data storage devices, such as USB drives and portable hard drives.

iii. Fail to properly secure laptops or other electronic devices used to access the school's data.

iv. Otherwise improperly or ineffectively dispose of electronic private educational or personnel records.

5. Redaction and Preventing Unauthorized Access.

a. Common Redaction Fails:

i. Using a redaction marker, but everything is revealed when you hold the document against the light.

ii. Using blacked-out word boxes on a PDF, but the boxes move when the file is sent, or the recipient can move the boxes because the document was not protected.

iii. Copying and pasting the redacted text. If redactions are done incorrectly, the pasted text will appear without any redactions.

iv. Failing to disable links to Google documents or ShareFile that contain private data.

v. Failing to "sanitize" your redacted document before sending, enabling individuals to access links that lead to documents containing private data.

b. Preventing Unauthorized Access to Private Data. Consider ways to establish appropriate security safeguards to prevent harm executed by hackers in today's high-tech world:

i. Strengthen password security.

ii. Avoid public Wi-Fi.

iii. Keep software and systems updated.

iv. Be aware of phishing emails.