

Board Data Practices Handout

STRIDE Academy • 2026–27 • Minnesota public charter school

Use this handout in a facilitated board training to practice protecting people's information while providing lawful public access. Members should leave knowing how to recognize protected data, route requests, preserve records, and respond to a possible disclosure.

What the assurance requires

MDE's 2026–27 Annual Charter School Assurances, item 7, addresses compliance with state data practices law, staff ability to report unethical or fraudulent actions, and board attendance at training that includes state data practices law. It asks for training dates and the most recent policy. This handout supports that training; distributing it does not establish attendance, completion, policy adoption, or compliance. [1]

Minn. Stat. §124E.07, subd. 7, requires new board members to complete data practices, open meeting law, and board-role training before beginning their term. A director or chief administrator serving ex officio must complete that training within three months of starting employment. Annual board training follows an assessment of training needs. The provider must certify individual completion; completed training belongs in the school's annual report. This module covers data practices, not every required training topic. [2]

Start with the legal classification

Charter schools must follow Chapter 13. Government data are public unless a law classifies them otherwise. Classification follows the information, not a "confidential" label, a personal email account, or a preference to avoid disclosure. [2–4]

Public. Accessible to anyone. Examples generally include adopted budgets, public minutes, and specified employee salary and job information.

Private data on individuals. Unavailable to the general public; accessible to the subject and others authorized by law. Student educational data and many personnel details fall here.

Confidential data on individuals. Unavailable to the public and to the subject. A specific law must supply this classification; "sensitive" alone is not enough.

For data not about individuals, the corresponding restricted categories are nonpublic and protected nonpublic. Ask the responsible authority to determine the applicable law and access rights. [3]

Board access has limits

A board seat does not give unrestricted access to student or employee files. Receive only data needed for authorized duties. Prefer aggregate reports; removing names may still leave a student identifiable in a small grade or subgroup. [5–7]

Protect people and preserve access

Student and personnel information

Student grades, discipline, disability and IEP information, school health records, and family information generally require protection. FERPA normally requires consent to disclose personally identifiable education records unless a permitted exception applies. School-official access requires a legitimate educational interest under the school's criteria. Let administration verify consent, identity, and authority. [5–6]

Directory information is not a blanket permission to share student information. Confirm STRIDE's actual designation, notice, opt-out status, and applicable restrictions before release. A parent discussing a child publicly does not authorize the board to disclose the school's records. [5–6]

Personnel files contain both public and private data. Names, salaries, job titles, and the existence and status of complaints are generally public; many evaluations, medical details, and complaint details are private. Final disciplinary dispositions have specific public-access rules. Do not release or withhold an entire file without review. [7]

When someone requests records

1. Preserve the request and responsive records. Promptly route the request to STRIDE's designated responsible authority or designee under its current public-access procedures. If the contact is unclear, ask the Executive Director's office to identify it. Do not assume any individual is formally designated. [4, 8]
2. Do not independently deny, promise secrecy, set fees, or send an unreviewed file. Public inspection is free; lawful copy fees and redaction are handled centrally. A public-data requester generally need not identify themselves or explain why they want the data. [4]
3. Treat deadlines seriously. Public requests require an appropriate, prompt response; copies are due as soon as reasonably possible. Data-subject requests have separate rules: access is immediate if possible, otherwise within 10 days, excluding weekends and legal holidays. Route parent/student requests promptly for identity and access review. [4, 9]

Emails texts and secure sharing

School-business email, texts, attachments, chats, and notes may be government data even on personal devices or accounts. Use school-approved systems, preserve responsive messages, and help retrieve them when requested. Do not use disappearing messages to avoid access or retention. [3, 10]

Before sharing, check recipients, permissions, and attachments. Use approved restricted-access channels for protected material. Keep it out of public packets, personal cloud storage, social media, and unapproved AI tools. Lock devices and secure paper copies. These are practical safeguards for the duty to protect data. [11]

Retention and possible breaches

Follow STRIDE's applicable approved retention schedule and any preservation hold. A record's public/private status does not determine when it may be destroyed. Do not delete responsive records to avoid a request; coordinate lawful disposal with administration. [2, 10]

Report a misdirected email, lost device, exposed link, or suspected unauthorized access immediately to administration and the designated data/privacy contact. Preserve evidence; follow containment directions. The responsible authority and counsel should evaluate required notices and investigation reporting under §13.055. Do not decide alone that recall or deletion resolves the incident. [12]

Practice the board response

Open meetings and protected data

Chapter 13 governs data access; Chapter 13D governs meetings. Private data alone do not authorize a closed meeting. Section 13D.05 requires closure for discussion of certain protected data, including nonpublic educational data, and permits or requires closure in other specified circumstances. Have the chair and counsel confirm the legal basis and required procedures before discussion. [13]

The law allows limited discussion of some nonpublic data when reasonably necessary for authorized board business, but this is not general permission to disclose student records. Use de-identified information when possible. Do not reproduce protected records in public packets or minutes without legal review. Avoid group-text or email deliberation that circumvents an open meeting. [13]

Staff reporting and nonretaliation

Staff must be able to raise unethical or fraudulent conduct through appropriate reporting channels. Minnesota's whistleblower law prohibits retaliation for specified good-faith reports of actual, suspected, or planned legal violations. Do not threaten, penalize, or obstruct a protected report, or promise absolute anonymity. Confidentiality rules do not justify silencing lawful reports; reporting protections also do not permit unlawful disclosure of protected data. If a report concerns the usual recipient, use an appropriate alternate channel such as the board chair or legal counsel. [1, 14]

Discuss before reading the responses

1 A parent asks for another child's discipline record

Do not confirm details or forward the record. Route the request for review. Another parent's interest does not establish authority to receive private educational data. [5–6]

2 A reporter requests board texts on your personal phone

Preserve school-business texts and route the request. The device does not remove the information from data-practices obligations; the content still needs classification review. [3–4]

3 A packet lists one student's IEP and test results

Stop publication and notify administration. Request an appropriately aggregated report. If already shared, report the incident immediately and preserve evidence. [5, 11–12]

4 A staff member reports suspected misuse of school funds

Preserve the report, avoid retaliation, and route it for appropriate review. Do not promise absolute confidentiality or distribute allegations broadly. [14]

5 A member proposes closing a meeting for a "personnel issue"

Ask for the specific legal basis first. Some proceedings must be open; others may or must close. The label does not decide the rule. [13]

Quick knowledge check

Can a confidentiality stamp change a record's legal classification? No.

Does a board seat allow access to every student file? No.

Does receiving this handout certify training completion? No.

Sources and training record

Prepared October 19, 2026. General training resource, not a legal opinion or adopted STRIDE policy. Apply current law and verified school procedures; consult the responsible authority or counsel on specific cases. Numbered references link to primary sources.

[1] MDE 2026–27 Annual Charter School Assurances, item 7

[2] Minn. Stat. §§124E.03, subd. 5, and 124E.07, subds. 7–8

[3] Minn. Stat. §13.02 — classifications and government data

[4] Minn. Stat. §13.03 — public access and requests

[5] Minn. Stat. §13.32 — educational data

[6] U.S. Department of Education — FERPA and school-official access

[7] Minn. Stat. §13.43 — personnel data

[8] Minn. Stat. §13.025 — access policies and contacts

[9] Minn. Stat. §13.04 — data-subject rights

[10] Minn. Stat. §138.17 — records management and disposal

[11] Minn. Stat. §13.05 — access and safeguards

[12] Minn. Stat. §13.055 — security breach requirements

[13] Minn. Stat. §§13D.01 and 13D.05 — meetings and protected data

[14] Minn. Stat. §181.932 — employee reporting protections

Additional direct links: [Board training law](#) • [Open meeting requirements](#) • [FERPA access FAQ](#)

Complete only after training occurs

Session date _____ Start/end time _____

Trainer and organization _____

Format/location _____

Participants completing training _____

Topics: classifications; student/personnel data; requests; security; retention; meeting boundaries; staff reporting; scenarios. Record any additional topics or follow-up needs:

Provider certification: I certify that the individuals listed above completed the training described in this record.

Trainer signature _____ Date _____

Retain this record, attendance evidence, materials, and any provider certificates. Enter only verified dates in the assurances and completed training in the annual report. Confirm the current policy attachment and responsible-authority contact separately. [1–2]