REQUIRED

FGA - STUDENT EDUCATION RECORDS AND PRIVACY

The **Hope-Page** School Board believes that while collection and use of student information is necessary to provide educational and student support services, the District must implement safeguards to ensure information is appropriately protected and used to serve the best interests of students. The purpose of this policy is to establish such safeguards.

Definitions

- *Directory information* is defined as personally identifiable information contained in a student education record that is generally considered not harmful or an invasion of privacy if disclosed and includes:

  a. Name (first and last)

  b. Address

  c. Dates of attendance

  d. Degrees, honors, and awards received

  e. Grade level

  f. Most recent school attended

  g. Participation in officially recognized activities and sports

  h. Photograph

  i. School email address

  j. Student identification number if it cannot be used alone to access an educational record and is not the student's social security number

  k. Telephone listing

  l. Weight and height of members of athletic teams

- *Education records* are records that are directly related to a student and are maintained by the District or by a party acting on behalf of the District. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records, and student discipline files. This definition excludes law enforcement records and records in the sole possession of the maker used only as a memory aid.
- *Eligible student* means a student who has reached the age of 18.

- *FERPA* stands for the Family Educational Rights and Privacy Act.
- *Legitimate educational interest* is defined as access that is needed in order for a school official to fulfill their professional responsibility.
- *Parent* means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.
- *Permanent record* is defined as a record containing a student's name, address, phone number, record of grades, years enrolled, courses attended, and grades completed.
- *Personally Identifiable Information* (PII) includes information maintained in the student's education record that could be used alone or in combination to trace a student's identity directly or indirectly and would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- *Record* means any information recorded in any way including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.
- *School official* is defined as an individual who has a legitimate educational interest in accessing student educational records and is affiliated with the District in one of the following capacities:

a. An individual employed by the District in an administrative, instructional, or support staff position;

b. School board members; or

c. Contractors, consultants, volunteers, service providers, or other party with whom the District has outsourced institutional services or functions for which the District would otherwise use employees; records provided to these third parties must remain directly under the district's control for purposes of maintenance and use and the third party must agree to comply with 34 C.F.R. 99.33(a). Examples include, but are not limited to, school resource officers, interns, student teachers, the district's attorney, PowerSchool, SLDS, learning management software, hot lunch tracking software, and district alert systems.

Designation and Responsibilities of Privacy Officers

The Superintendent or designee shall serve as Chief Privacy Officer. In this role, the Superintendent is responsible for submitting to the Board for approval student information sharing requests from third-party individuals/entities other than parties to which the District reports student information under law. The Superintendent shall also maintain a master list of individuals and entities having access to student information, including school district personnel listed by title. To ensure this list remains current and is manageable to maintain, it shall not contain names of individuals who have access to data.

The Superintendent may designate privacy officers at the District and building level. These privacy officers are responsible for:

1. Maintaining a list of school personnel by title who have access to student information; this list shall be provided to the Superintendent each time it is updated;
2. Submitting to the Superintendent for board approval new requests to share student information with third-party individuals and entities other than parties to which the District reports student information under law;
3. Ensuring that access to student information is granted only to the extent there is a legitimate educational interest and in accordance with this policy and any applicable agreements;
4. Enforcing this and other applicable district confidentiality and data protection policies; and
5. Providing a list of students who have opted-out of directory information to classroom teachers and other district staff who have a need to know.

REQUIRED

Information Release Safeguards

1. Access by Parents and Eligible Students

To ensure compliance with parental and eligible student access requirements under FERPA:

a. The District shall comply with a request by a parent or eligible student to access education records within a reasonable period of time, not to exceed 45 days after receipt of a request; and

b. The Board shall develop procedures for a parent or eligible student to review and amend educational records. These procedures shall include procedures to verify the identity of a requesting parent or eligible student. The regulations shall be delineated in board regulations and disseminated annually in accordance with law.

2. Classroom Use of Instructional Tools Requiring Release of Student Information

Teachers are encouraged to use instructional technological tools that allow for use of an alias or that do not require submission of directory information, other than or in addition to name, or PII. Whenever a teacher wishes to use an instructional tool that requires release of directory information, other than or in addition to name, or PII such as, but not limited to, software or an app, the teacher shall submit a request to the building-level privacy officer. The privacy officer shall check the district's master list of individuals and entities approved to receive student information. If the entity is not on this list or the teacher's request

is beyond the scope of information sharing permission previously granted, the privacy officer shall either deny the teacher's request or submit an information-sharing request to the Superintendent for board approval. If the teacher is authorized to use the instructional tool, the building-level privacy officer shall ensure the teacher complies with any parental consent requirements and directory information opt-out requests before using the tool.

3. Data Breaches

District employees are responsible for informing a privacy officer of any known or suspected breach of PII. When a privacy officer becomes aware of a breach of student PII, they shall contact the Chief Privacy Officer. The Chief Privacy Officer shall determine if enactment of data breach response procedures contained in policy IDC and NDCC Ch. 51-30 is appropriate.

4. Information Storage and Destruction

Student education records shall be reviewed annually and any records unnecessary for progression to the next grade level, not needed for college entrance purposes, not needed for extracurricular participation, not needed for disciplinary purposes, and records that are not part of the permanent record will be shredded or destroyed. Exceptions apply for any content that may reasonably be related to litigation or anticipated litigation (retain for six years after a student turns eighteen), bullying reports (retain in accordance with policy ACEA), concussion documentation (retain in accordance with policy FCAF), executive session tapes (retain for at least six months), PowerSchool records, and special education records (retain in accordance with the Individuals with Disabilities Education Act).

5. Directory Information

The District may disclose directory information without parental or eligible student consent if it has given parents or eligible students a reasonable amount of time to opt-out of directory information release. Opt-out notices should be provided at the beginning of the school year and when a student otherwise enrolls in the District. These notices shall contain a reasonable deadline of at least ten days for parents or eligible students to opt out.

The Board approves release of directory information as follows:

a. To board-approved vendors for purposes of sale of school-related items such as, but not limited to, yearbooks, school pictures, graduation items, district apparel, and book orders;

b. To military and college recruiters in accordance with applicable laws (NDCC 15.1-07-25.1 and 20 U.S.C. 7908);

c. To official district newspaper for purposes of recognizing student accomplishments and coverage of extracurricular events;

d. To school-affiliated groups for purposes of communicating and fundraising;

e. To school-sponsored student publications including, but not limited to, newspapers and yearbooks; and

f. When the Board receives and approves a directory information release request; directory information shall only be released and used for purposes specified in the release request and the Superintendent shall add approved requestors to the district's master list of individuals and entities having access to student information. The Board shall develop criteria in regulations for approving and denying these requests.

Any district employee who wishes to disseminate student directory information to a third party shall contact their building-level privacy officer. The privacy officer shall determine if the Board has previously approved such release and, if not, deny the request or submit it to the Superintendent for board approval. Upon board approval, the Superintendent shall instruct the privacy officer to ensure compliance with any opt-out requests made by parents.

6. Personally Identifiable Information (PII)

Any third party requesting or receiving access to student PII must receive board approval unless the third party is required to receive PII under state or federal law. Any school employee who wishes to share PII with a third party shall contact their building-level privacy officer. The privacy officer shall determine if the Board has previously approved such release and, if not, deny the request or submit it to the Superintendent for board approval. Upon board approval of any PII release request, the applicable privacy officer shall inform the requestor of any parental consent requirements (see #7) and ensure the requestor complies with such requirements.

Parental or eligible student consent is not required to release PII under the following circumstances:

a. The District receives information under 42 U.S.C. 14071 and applicable federal guidelines about a student who is a registered sex offender under section 170101 of the Violent Crime Control and Law Enforcement Act of 1994 (42 U.S.C. 14071), and the District has a need to disclose the student's status as a sex offender for safety purposes;

b. In connection with a health or safety emergency under the conditions described in 34 C.F.R. 99.36;

c. If records have been de-identified by the District; third party individuals and entities that receive de-identified information shall be included on the district's master list of individuals and entities having access to student information

d. To a school official who has a legitimate educational interest in the education records if the following conditions are satisfied:

i. Access shall be limited to only information the school official has a legitimate need to know;

ii. School officials shall use the information only for the purposes for which the disclosure was made and shall not re-disclose the information to any other party without proper consent or legal authority; and

iii. Titles of individuals and entities considered school officials shall be included on the district's master list of individuals and entities having access to student information;

e. To a court without a court order or subpoena when the District initiates legal action against a parent/student or a parent/student initiates legal action against the District

f. To accrediting bodies for purposes of accreditation

g. To an organization conducting a study for the District to develop, validate, or administer a predictive test; administer student aid programs; or improve instruction so long as the organization has entered into a written agreement with the Board in accordance with law; if the organization is conducting a survey of students, the District shall ensure parents are notified in compliance with policy GCC and shall obtain parental consent, if applicable (see #7)

h. To another school in which the student seeks, intends to, or is already enrolled

i. To authorized representatives of the Comptroller General of the United States, the Attorney General of the United States, the U.S. Secretary of Education, and state and local educational authorities for audit or evaluation of federal or state supported education programs or for the enforcement of or compliance with federal legal requirements that relate to those programs;

j. To comply with a judicial order or lawfully issued subpoena; the District must make reasonable attempt to contact the parent or eligible student before disclosure unless the court order instructs otherwise;

k. To the parents of an eligible student who is also a "dependent student" as defined in IRS Section 152; or

l. To the state entity managing a student information system so long as the organization has entered into a written agreement with the Board in accordance with law; the data sharing agreement must include a clause that designates the department as an authorized representative of the District under FERPA for purposes of the statewide longitudinal data system.

The District will take measures necessary to ensure that individuals and entities to which PII is released shall only have access to information necessary to fulfill

their responsibilities under law and to the District. Measures may include, but not be limited to, controlling access to computer data through password restrictions, controlled access to paper records, and ensuring that any information access agreements required by law are properly executed by the Board.

7. When Parental Consent is Required

The District must obtain parental or eligible student consent to release student information under the following circumstances:

a. The Board has approved release of PII to an individual or entity not meeting the definition of school official under law and/or not meeting an exception to the parental consent requirement under FERPA;

b. The Board has approved release of directory information, other than or in addition to name, or PII to an online service provider for commercial purposes and the impacted students are under the age of 13;[1][1]

c. When administering a survey funded in whole or in part by the U.S. Department of Education and concerning any of the following areas[2][2]:

   i. Political affiliations or beliefs of the student or the student's parent;

   ii. Mental or psychological problems of the student or the student's family;

   iii. Sex behavior or attitudes;

   iv. Illegal, anti-social, self-incriminating, or demeaning behavior;

   v. Critical appraisals of other individuals with whom respondents have close family relationships;

   vi. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

   vii. Religious practices, affiliations, or beliefs of the student or student's parent; or

   viii. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

If the District is unable to obtain this consent, it shall not release the impacted student's information.

504 Plans and Individual Educational Programs (IEPs)
Sharing of student information necessary for developing, amending, or implementing an IEP or 504 Plan and sharing student information needed to determine eligibility for special education or disability services are not subject to board approval requirements

in NDCC 15.1-07-25.3 because the District provides these services in fulfillment of requirements under state and federal law.

Policy Violations
Failure by a district employee or volunteer to comply with this policy, other district confidentiality requirements, or any improper disclosure of student information by a school employee or volunteer shall result in disciplinary action up to and including termination of employment. Failure by a third party to comply with this policy, any information-sharing agreements between the District and third party, or any improper disclosure of student information by the third party may result in termination of the third-party's access to student information and termination of the district's agreement with the third party.

Training
School officials employed or volunteering for the District shall receive information and/or training on confidentiality requirements pertaining to student education records and consequences for breaching confidentiality. The District shall also provide training to applicable school personnel on the procedures for requesting to release student information contained in this policy.

Complementing NDSBA Templates (may contain items not adopted by the Board)

- DE, Staff Code of Conduct
- FACB, Transfer and Withdrawal Records
- FGA-BR1, Student Education Records Access and Amendment Procedure
- FGA-BR2, Criteria for Approving and Denying Directory Information and PII Release Requests
- FGA-E1, Notice for Directory Information
- FGA-E2, Model Notice of Rights Under FERPA for Elementary and Secondary Schools
- FGA-E3, FERPA Release Form for Parents
- FGA-E4, Notice of Executive Session Tape on File
- FGA-E5, Student Information Sharing Request
- FGA-E6, Model Form for Disclosure to Parents of Dependent Students
- FGA-E7, School Officials' Guide to FERPA and Data Privacy
- FGA-E8, Parties Approved to Receive Student Data

- GCC, Protection of Pupil Rights Amendment and Third-Party Research on Students
- IDC, Data Protection and Security Breaches

Legal References

- 20 U.S.C. § 1232g, Family Education and Privacy Rights
- 34 CFR Part 99, Family Educational Rights and Privacy
- NDCC § 15.1-06-06, Approval of Public Schools
- NDCC § 15.1-07-25.3, Protection of Student Data – School District Policy
- NDCC § 15.1-07-33, Student Information System - Exemption
- NDCC § 15.1-19-14, School Law Enforcement Unit
- NDCC § 15.1-19-15, Record Retention

End of Hope-Page Policy FGA . . . . . Adopted: 07/2025

---

[1] Children's Online Privacy Protection Act, 16 CFR 312
[2] Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h; 34 CFR Part 98