A Briefing on Student Information

Safeguarding Privacy:

You are responsible

Anoka-Hennepin School District employees, volunteers and others working on behalf of the district who use student data are responsible for protecting student privacy. This responsibility extends to the access, use, release and disposal of any information on students.

This document is an overview

This document is designed to provide Anoka-Hennepin employees with general guidelines about protecting student privacy. It does not address all of the laws and policies related to student records and data privacy. For more information on student data, contact your principal/supervisor, Director of Technology and Information Services, or the District General Counsel.

Anoka-Hennepin’s Student Records Policy is available on-line at www.anoka.k12.mn.us. Go to the School Board section and click on School Board Policies. (500 students)
Your role in safeguarding student privacy

Administrators, teachers, counselors, substitutes, support staff, temporary workers, or outside agency staff may have access to selected student information on a need to know basis, and/or pursuant to law.

“Directory Information” is public information

All data on students maintained by the school district, or by persons acting for the school district are private. The only exception is “directory information,” which has been designated by the district as public information.*

Directory information is:

- Name and photo.
- Name of school(s) attended.
- Date of birth.
- Grade in school.
- Participation in officially recognized activities and sports.
- Awards and honors.
- Weight and height of members of athletic team.
- Dates of attendance (enrollment dates).
- Last grade completed.
- Date of graduation.
- Immunization history.

*Parents/guardians may restrict directory information by notifying the district in writing.

Desk Drawer Exception

Records maintained by instructional personnel which are in their sole possession and are not accessible or revealed to any other individual except a substitute teacher and are destroyed at the end of the school year are not considered to be public data.

Written permission required

With some limited exceptions, all agencies (such as post-secondary schools, employers, social agencies, police) or persons (including grandparents) must have written permission from the parent/guardian in order to gain access to the student’s records (except for directory information).

Student Information - What is it?

Student information is all data (paper and electronic), collected and maintained by school district, which relates to the individual student.

- No one may access private student information unless the employee’s work assignment requires it.
- Student information must be used to further the educational needs of students.

Privacy is a legal and professional expectation

- Keeping student information confidential is vital to professionalism.
- The federal Family Education Rights and Privacy Act (FERPA) and the Minnesota Government Data Practices Act (MGDPA) mandates the privacy of student information.
- The code of ethics for Minnesota teachers states that “a teacher shall disclose confidential information about an individual only when a compelling professional purpose is served or when required by law.”
- Failure to safeguard student information may result in disciplinary action.

Be careful what you share

Student information must remain confidential in all communications; oral, written and electronic. Under no circumstance should private information be the topic of conversation in a public space, including public forums on the Internet. Any information acquired regarding a student while working in a school or while assisting at school functions should be kept confidential. Personally identifiable information must never be discussed with friends, neighbors or family.

Important reminders

- Keep confidential all student information unless classified as directory information, and the student has not opted out of directory information.
- Be especially cautious about the inadvertent release of student information, e.g. leaving a document with private information on a desk or open on a computer.
- Keep electronic devices such as cell phones and iPads secure and access-password protected.
- Protect viewability of computer screens and lock access when away from your work station.
- Immediately retrieve printed material.
- Information that identifies any individual student must be disposed of properly (i.e. shredded).