# FERPA REFERENCE SHEET

The Family Educational Rights and Privacy Act of 1974, as amended (**FERPA**) requires institutions accepting federal monies to protect the privacy of student information. In addition, FERPA affords students the right to review their education records, to request correction of inaccurate records, and to limit information disclosure from those records. An institution's failure to comply with FERPA may result in the Department of Education withdrawal of federal funds.

As a DMPS staff member, you are allowed access to a student's educational records if you need the information to fulfill a specific professional responsibility. To protect the privacy of students, you need to know the difference between **Directory Information** and **Non-Directory Personally Identifiable Information (PII)** within **Education Records**.

## Education Records

Records directly relating to a student that are maintained by the school or by a third party* that the school enlists for certain functions.
* For example, a company that provides course management software.

### Directory Information

Educational records that are generally not considered harmful to students if publicly released.

- Name
- Current mailing address
- Current telephone number
- Parent/guardian e-mail address
- School
- Grade level
- Dates of enrollment
- A full list of directory information is located here

**This information may be disclosed, unless a parent/guardian has requested otherwise.** *Please refer such requests to your school's office manager.*

### Non-Directory Personally Identifiable Information

Educational records that are more sensitive than directory information (any identifying data other than directory information). Including, but not limited to:

- Student ID
- Gender
- Race/ethnicity
- Meal status
- Class schedule
- Grades/GPA
- Test scores
- Academic transcripts
- Attendance
- Behavior referrals
- Student work/assignments

**Under FERPA, this information CAN NOT be disclosed without parental/guardian consent.**

## General Practices for Protecting Student Information and Education Records

| DO | DO NOT |
| --- | --- |
| • ONLY access information specific to your duties.<br>• ALWAYS lock computer screens when leaving your workspace, even if only for a moment.<br>• ALWAYS use encryption when emailing student information.<br>• DO ask yourself when sharing student information:<br>  ○ Can someone personally identify the student from this information?<br>  ○ Do I have parental consent?<br>• DO check on Infinite Campus to see if any parents/guardians have told the school not to share their child's directory information.<br>• DO shred student documents before disposal.<br>• DO use educational technology preapproved by your school.<br>• DO check for parental consent before including non-directory information in a student recommendation. | • DO NOT save student information on unprotected or personal drives/devices.<br>• DO NOT leave documents with sensitive information lying around in plain sight.<br>• DO NOT share your password.<br>• DO NOT allow a student's grade to be exposed to any student other than to whom they belong.<br>• DO NOT access student information unless there is a specific and legitimate educationally related need.<br>• DO NOT share non-directory student information with coworkers unless necessary.<br>• DO NOT use educational technology programs that your school does not have a contract for. Check with your school administration if you are unsure whether a contract exists for a particular program.<br>• DO NOT publicly post students' personal information online without parental consent.<br>• DO NOT use social networks to connect students with classroom pages and events without parental consent. |


You may disclose non-directory information in an **emergency.** That is, when it is necessary to protect the health and safety of student(s).