

Controlled Reports and PII

Last Modified on 05/09/2024 11:26 am CDT

[Understanding PII](#) | [Identifying Reports Containing PII](#) | [Who Can See PII](#) | [Additional Precautions to Protect PII](#)

Understanding PII

PII (Personal Identifiable Information) is any private or sensitive information that can be used to identify an individual personally. As a Student Information System, Infinite Campus has many locations where PII data exists. To protect this information, every tool and report in Campus is guarded by set of [tool](#) and [calendar](#) rights to prevent unauthorized access. However, even with strong safety measures in place, PII can still be compromised if a user does not do their part to keep sensitive data secure. It is critical that every Campus user understand the role they play in protecting PII.

Personal Impacts when PII is compromised

Fraudulent activity such as identity theft can cause substantial damages to a person if their PII is compromised. PII is considered compromised when a person has gained access to information they are not authorized to access. Once compromised, PII can be used for:

- Opening a new credit card or loan
- Opening a bank account
- Other fraudulent activities

Examples of PII include:

- Social Security Numbers
- Birth Dates
- Physical Addresses
- Other forms of ID a person may use

In Campus, PII is viewable in areas such as Demographics and Census. Data in these locations may be used in state reports and is available for extraction using Ad hoc Reporting.

PII Examples

Student, Frankie L.

Gender: F

Nickname: [Redacted]

Race Ethnicity: 01: American Indian or Alaskan Native

Federal Designation: 2: American Indian or Alaska Native

Race(s): American Indian or Alaska Native

Hispanic/Latino: N: No

Race/Ethnicity Determination: [Redacted]

Birth Date (Age: 18): 03/03/2003

Student Number: 679

State ID: [Redacted]

NASIS ID: 55555555

Person GUID: BAC339BF-F658-4098-8799-0B2AE3CE2C2C

Contact Information

Other Phone: (715)555-5555x137

Cell Phone: (715)555-5555x789

Mailing Addresses

Primary Address: 10 2ND CIRCLE LOOP, Campus, MN 59864

Student **Primary

Household Phone: (726)555-5555x111

Address: 10 2ND CIRCLE LOOP, Campus, MN 59864

Name	Relationship	Enrollment (grade)	Contact Method
Student, Frankie L	Self	20-21 High School (12)	Oth: (715)555-5555x137 C: (715)555-5555x789
Second Circle, Bryan Parent	Second Circle(guardian)		

Non-Household Relationships

Name	Relationship	Contact Method

Examples of PII

Identifying Reports Containing PII

Many reports available on Campus include PII for the purposes of accurate reporting and identification. As a precautionary measure, **BIE** and **NASIS** reports containing PII display a **CONTROLLED** security statement in the report header for PDF and DOCX formats. For CSV and TXT formats, a file name indicating Controlled Unclassified Information (CUI) is included in the report. CSV formatted reports with PII are named *SampleReport_CUI.csv*. A; while reports in TXT format that include PII are labeled *SampleReport_CUI.txt*.

Users should follow their school district's policy when viewing reports where CONTROLLED displays and where the file name indicates PII exists.

The **CONTROLLED** statement only displays in reports containing PII for BIE schools and NASIS.

River School District PO Box 1, Pablo, MT 59855 Generated on 06/29/2021 01:27:52 PM Page 1 of 1		Student Enrollment Summary Report Effective Date: 06/29/2021 Enrollment Types: P, S, N Total Race/Ethnicities: 2 of 7 Total Schools: 1 Race/Ethnicity Source: Federal Male/Female/Total: 57/55/112						
CONTROLLED: This page contains PII and should be handled to protect privacy.								
Student Population by Race/Ethnicity and Grade Level (Male/Female/Total)								
River School								
Grade	1:Hispanic/Latino	2:American Indian or Alaska Native	3:Asian	4:Black or African American	5:Native Hawaiian or Other Pacific Islander	6:White	7:Two or more races	Total
08	-	6/7/13	-	-	-	-	-	6/7/13
09	-	0/1/1	-	-	-	-	-	0/1/1
10	-	7/11/18	-	-	-	-	-	7/11/18
11	1/0/1	10/12/22	-	-	-	-	-	11/12/23
12	2/0/2	31/24/55	-	-	-	-	-	33/24/57
All Grades	3/0/3	54/55/109	-	-	-	-	-	57/55/112
Student Population Excluding White not of Hispanic Origin								
School			Total			Percentage		
River School			112			100.00%		

Example of "CONTROLLED" in a Report Header

Who Can See PII

Authorized Users

Anyone assigned tool rights to view student data or generate reports in Campus may be eligible to see the PII of students, staff, and others (parents, guardians, emergency contacts, etc.). When viewing PII, it is important to review and follow the policies enforced by your school district.

Unauthorized Users

Unauthorized users are individuals who do not have permission to access the information to which they have gained access. Unauthorized users may gain access when PII handling negligence occurs by an authorized user. Examples of PII negligence include:

- Not locking your workstation before leaving it unattended
- Sharing your username and password
- Printing a **Controlled** report and leaving it in an area where unauthorized users may see it
- Improperly disposing of documents containing PII

Additional Precautions to Protect PII

It is important to always follow your school district's policies when viewing or working with PII. Below are a few examples of how you can help to reduce the risk of compromising PII:

All Users:

- Never leave your workstation unattended when PII is displayed or can be easily accessed. Consider locking your computer even when trips away from it are brief.
- Never leave a printed report that contains PII in a location where it can be stolen, including

sitting on a communal printer.

- Never provide your password to another user with restricted or fewer tool rights than you.
- Never save a downloaded report containing PII on a shared server where others can see it.

Administrative Users:

- Review and assign only the tool rights a user needs to perform their job tasks.
 - Restrict who is authorized to be given the Student Information System Administrative role.
 - Disable user accounts for employees who have left the organization.
 - Review tool rights for employees changing roles in the school/district.
-