Student Data Privacy

To maintain the confidentiality and integrity of the District information and data including our student data, the District's Technology Services department has implemented targeted processes and procedures.
These can be categorized as:

- Systems that control where key information is stored.
- Access security practices and internal controls that restrict who has rights to view, add/delete or edit information.
- Physical access controls to District data centers and key networking equipment.
- Data Services Agreement to ensure data is secured with external solution providers.

How is access to student data managed?

District 214 follows best practices in establishing and managing system and network access security. An Information Security Policy governs all access and control measures to protect District data. Access to student data is managed and controlled through what is known as role-based security. This means that the type and amount of access to student data and other information is governed in our systems by the role which any staff member holds in the District along with what information they require to perform their job. Staff members must go through a process to gain access to authorized information that includes successfully logging into the District network or one of the systems they use as part of their job duties.

District 214's authentication requires staff to use their District assigned Active Directory username and password or an application specific username and password to gain access to functionality and data residing in our systems. These usernames and passwords are specific to individual staff or system users. Once a staff member logs in using this method the internal application controls role based security. Application permission restrictions are engaged which limit the data read, write, add or delete functionality and are specific to a staff member's role in the District. This process is also used by our District 214 parents/guardians when accessing information specific to their students in any of our systems.

The district also follows all rules set forth by state and federal government such as the Federal Educational Rights and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA), and the Health Insurance Portability and Accountability Act (HIPAA). For more information regarding these laws, please refer to the following links:

http://www.hhs.gov/ocr/privacy/index.html
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
http://familypolicy.ed.gov/ppra

Where is student data held and where does it go?

The primary repository of student data is our Student Information System, Infinite Campus. Infinite Campus maintains student demographics, household contact information, enrollments, attendance, grades, schedules, transcripts, discipline, bus, lockers, health, and LEP information. ***The District does not retain student Social***

Security Numbers within any system. In addition to the Infinite Campus system, the Technology Services department also maintains multiple supporting systems that assist in running the daily operations of the District. Based on need, some excerpts of student data are routinely transferred between these applications through a variety of secure and encrypted system integration processes. Additionally, many of these applications are internally hosted in our secure primary and secondary data centers. Physical access to these data centers and the servers that house this data is limited to a small group of network and application administrators in the Technology Services department. D214 data centers are secured, include fire protection and power backup capabilities. Routine back-ups of key systems and data are processed on a regular schedule, which are securely stored and protected.

With the evolution of Cloud-based applications, the District also subscribes to some externally hosted applications which are integrated with our Student Information System through encrypted data communications. Below is a list of some of the various outside agencies that the district provides data to, and or receives data from, via secured, encrypted data transfer interfaces.

- **Regular basis** - Learning Management System (Schoology), District Assessment Management system (Mastery Manager), Library Management System (Follett), Food Service Point of Sale, and mass notification system (School Messenger). Data transferred includes basic student information such as student names, student schedules, teachers, and teacher schedules.
- **Periodic basis** - Testing agencies such as ACCESS, ACT, AP, ASFAB, PARCC, PSAT, and SAT. These tests typically include basic student demographics to identify the student and student schedules used for test scheduling purposes.
- **Occasional basis** – Military, picture companies (LifeTouch), fundraising (Booster Clubs, D214 Foundation, etc.), institutions of higher education, and The Illinois High School Association (IHSA), which typically contains basic student information only.
- **Government entities** – Required data is shared on a daily, weekly, monthly, quarterly, and annual basis to the Illinois State Board of Education (ISBE). The Department of Education Office of Civil Rights requires the District to supply various data and/or reports. This data can contain detailed student demographic data, enrollment data, discipline data, grades, IEP, 504, LEP, and Free and Reduced Lunch information.

If problems occur that require application support personnel from one of the District’s solution providers, access to these applications by the vendor is granted to correct issues or perform system maintenance and upgrades.

Data Services Agreement

The District has established non-disclosure agreements with vendors as well as having information confidentiality language included in the Data Services Agreements. Additionally, when selecting new vendors the District requires that the vendor have a secure data transfer process, physically secured data centers, role-based security, and contract language that addresses information confidentiality and non-disclosure clauses.