Data Privacy

Helping Protect Staff and Students

Personal Identifiable Information (PII)

Personally Identifiable Information - also known as “PII” is considered sensitive information and must be safeguarded. Personally Identifiable Information includes an individual’s first name or initial and last name along with data elements such as social security number, medical information, health information, educational records or any unique identification need to be protected.

This presentation is designed to help staff have a better understanding of procedures, policies and laws that are in place to help protect data.

Directory Information

Data that is defined as “Directory Information” by board policy is not considered Personal Identifiable Information but caution and best practices should still be used when utilizing the data.

Directory Information is defined in board policy JO (Student Records) and includes but is not limited to student's name; parent's name; address; telephone number; date and place of birth; major field of study; grade level; participation in officially recognized activities and sports; weight and height of members of athletic teams; athletic performance data; dates of attendance; degrees, honors and awards received.

Proper Handling of Data

Only access student and/or employee data when necessary to accomplish your work requirements.

- Ensure data is properly secured
- Lock filing cabinets when not actively in use
- Computers are locked when you are away from them
- Applications, e.g. Power School, Special Education programs, etc. are logged out when not in use
- If you find that you have access to data that isn't required for your position, notify your administration or call the Help Desk at x7078.

Applicable Policies and Laws

To help protect data, the following District policies are in place for review.

- JO: Student Records
- EHB: Technology Usage
- EHBC: Data Governance and Security

The District must also follow laws that include but are not limited to:

- FERPA
- COPPA
- CIPA
- PPRA

Applicable Policies and Laws

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children.

Applicable Policies and Laws

CIPA: The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program.

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

Online Services and Applications

With board policy EHBC (Data Governance and Security) and various federal laws, the District must vet online services and applications in order to help protect student data.

District provided services and applications have been evaluated and are safe for staff members to use. However, staff members who would like to utilize a service or program that requires a student logon or has access to student data, must have the program evaluated prior to use.

Vetting Online Services and Applications

If there is a service or program that requires students to logon or has access to student data and is not District provided, please follow the following steps.

- Goto http://lps53.org/technology and view the Web Resource Approval Flowchart.
- The flowchart will guide you through a series of scenarios and identify when it is safe to use a resource and when an application request must be submitted.
- If an application needs to be submitted, click on the Instructional Pilot/Web Resource Application link in the flowchart.

Summary

- You should only access data that is needed to complete your assigned job function.
- Special care should be taken when handling student/staff data.
- The use of some services and applications require a vetting process first.
- Everyone is a data custodian and is responsible for the security of Liberty's data by following data policies.
- If you are unsure about the District's data policies or have questions, contact your building administrator or the Help Desk.