Louisiana Department of Education **Employee Policies**
Special School District (SSD) **Effective Date: August, 2015**

Collection and Release of Personally Identifiable Student Information

****

Philosophy

In order to educate students, certain personally identifiable information must be collected and maintained. The privacy of personally identifiable student information is protected by federal law through the Family Educational Rights and Privacy Act (FERPA). The State of Louisiana has determined that personally identifiable information is protected as a right of privacy under the Constitutions of Louisiana and the United States and also provides for privacy protection through state law.

Definitions

"Parent" or "Legal guardian" means a student's parent, legal guardian, or other person or entity responsible for the student, which may include a student who has been emancipated or reached the age of majority.

"Personally identifiable information" is information about an individual that can be used on its own or with other information to identify, contact, or locate a single individual, including but not limited to the following:

- Any information that can be used to distinguish or trace an individual's identity such as full name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information.
- Two or more pieces of information that separately or when linked together can be used to reasonably ascertain the identity of the person.

Policy

Everyone must protect any and all student information that is available or entrusted to them. This includes protecting any electronic or paper files, flash drives, computers, briefcases, and other items or devices that contain personally identifiable student information, from unauthorized access.

Employees may release personally identifiable student information under the following circumstances:

- To report child abuse or neglect, as provided by law
- When permission is given by the SSD or LSS Superintendent, the School Director or Principal, the Director of Academic Services, the Director of Non-Academic Services, or the SSP Chief Academic Officer

When any employee receives a request to release student information, the employee must forward the request to the School Director, the Director of Academic Services, the Director of Non-Academic Service, or the SSP Chief Academic Officer for approval before releasing the information.

- This does not apply to a parent's request for information during a meeting, such as an IEP meeting.

If any employee believes students would benefit from anything that requires students' personally identifiable information (which could include web services or software, whether free or purchased by the school or an employee, or even awards or recognition for students), the employee must get approval from the School Director or the Director of Student Services before providing the students' information.

Any program or activity that requires personally identifiable student information be provided must be approved by the School Director (if limited to a single LSS school), the Director of Academic Services the Director of Non-Academic Services, or the SSP Chief Academic Officer, and must have an agreement that provides for student privacy. If personally identifiable student information may be transferred to the recipient's computers, the approval will only be made after consultation with the IT Director. Any agreement which requires funding must also be approved through the regular purchasing process.

Each School Director, the Director of Academic Services, the Director of Non-Academic Services, and the SSP Chief Academic Officer must maintain a list of people or entities to which personally identifiable student information is sent, and must send the list, and updates to it, to the Student Data Manager, who will be responsible for maintaining a comprehensive list. The Student Data Manager will provide information to the IT Director, who will maintain a list of entities to which personally identifiable information is sent electronically. These lists need not include other school districts to which information is sent in accordance with La. R.S. 17:112, people or entities to which information is given only after a parent requests it (such as colleges or LHSAA).

No employee may sell, transfer, share, or process any student data for use in commercial advertising, or marketing, or any other commercial purpose. This restriction does not apply when an employee is the parent.

<u>Personally Identifiable Student Information Stored on District Computer Systems</u>

Personally identifiable student information stored on SSD's computer systems is only available as follows:

- To a person authorized by the state to audit student records
- To a person authorized by the Superintendent to maintain or repair the computer system or to provide services that SSD would otherwise provide
- For each school:
    - A student who has reached the age of eighteen or is judicially emancipated or emancipated by marriage may access his or her own records.
    - The parent or legal guardian of a student who is under the age of eighteen and not emancipated may access that student's records.
    - A student who has reached the age of eighteen or is emancipated and the parent or legal guardian of a student who is under the age of eighteen and not emancipated may authorize another person, in writing, to access information about that student.

- Teachers of record may access their current students' records.
- School Directors, Principals, and Regional Coordinators may access the records of students in their schools.
- Assistant Principals may access the records of students in their schools and of students who are served by employees they supervise. (This may be necessary when a middle school student takes a high school course, for example.)
- The School Director, Principal, or Regional Coordinator may authorize employees in their schools to access student records, only to the extent necessary to perform their duties.
- The following employees may access computer systems on which information for students from both LSD and LSVI is stored: The SSD and LSS Superintendents, the Director of Academic Services, and the Director of Non-Academic Services, to the extent necessary to perform their duties
- The Superintendent may authorize access for other employees, only to the extent necessary to perform their duties.
- The Director of Academic Services or the Director of Non-Academic Services may authorize other employees in their Divisions to access student records, only to the extent necessary to perform their duties.

- The following employees may access computer systems on which information for students from throughout SSP is stored:
  - The SSD Superintendent and the SSP Chief Academic Officer, to the extent necessary to perform their duties
  - The SSD Superintendent and the SSP Chief Academic Officer may authorize access for other SSP employees, only to the extent necessary to perform their duties.

Any person authorized to access the computer system, other than the parent or legal guardian, shall maintain the confidentiality of all information to which access is granted. Failure to maintain confidentiality is punishable as provided by law.

The IT Director will maintain a list of all employees and others who have been given authority to access student records maintained by SSD's computer systems and will be responsible for removing access when it is no longer required for those people to perform their duties.

The administrator who granted access will be responsible for informing the IT Director when access is no longer needed.

Personally identifiable student data may not be stored on shared drives, unless specifically authorized by the Superintendent, the Director of Academic Services, the Director of Non-Academic Services, the School Director, or the Principal, as appropriate. Any employee who finds personally identifiable data stored on shared drives must report to the appropriate listed administrator for removal or for authorization.

Restrictions Not Intended to Interfere with Performance of Duties

These restrictions are intended to protect students and their families, and not to prohibit employees from performing their duties to serve students. If these restrictions interfere with the performance of an employee's duties, the employee should consult the employee's immediate supervisor immediately.

Reporting Unauthorized Release of Personally Identifiable Student Information

Any employee who reasonably believes that personally identifiable has been released without authorization must report the release to the School Director or to the employee's Division Director.

Penalties

Employees who violate the privacy of students' personally identifiable information are subject to disciplinary action or termination.

Anyone who violates any provision of law related to privacy of personally identifiable student information may be punished by imprisonment and/or fine.