INFORMATION AND DATA SECURITY POLICY

Background and Purpose

The provisions of the Information and Data Security Policy detail the responsibilities of Lafayette Parish School System employees in maintaining the security of non-public information used for administrative purposes. These individuals are also subject to the policies contained in Policy File: GAM—Electronic Resources Policy.

Administrative information requires responsible use by members of the Lafayette Parish School System (LPSS) community. The risk to the school district, its students, employees, and clients posed by data loss and identity theft is of significant concern to the Lafayette Parish School Board and can only be reduced through the combined efforts of every employee and contractor. Employees are expected to act in a manner that will ensure information, which they are authorized to access, is protected from unauthorized access, unauthorized use, invalid changes, and/or destruction.

The school district adopts this policy concerning sensitive information to help protect the students, employees, and their families from damages related to the loss or misuse of sensitive information. This policy applies to employees, contractors, consultants, and temporary workers.

Definition of Non-Public Information (NPI)

This policy refers frequently to "non-public information" (NPI). NPI includes the following items, whether in electronic or printed format:

- Social security number
- Driver's license number, particularly when found in combination with the individual's name and date of birth
- Medical information, including but not limited to, a person's doctor; insurance claims; prescriptions; or any related personal medical information
- Employee references and evaluations
- Individual Education Plans (IEPs) for special education students
- Student grade records and standardized test data
- Student discipline records
- Student evaluation and assessment results
- Student driver training records
- Student health records
- Any other student records in the cumulative folder except directory information as defined in Policy File: JR

Documents containing NPI are also referred to in this policy as "sensitive documents" or "confidential documents."

Access to Documents Containing NPI

Prior to a new employee receiving access to records containing NPI, the individual's supervisor must authorize in writing the new employee's necessity of access and level of access to this information. New employees must be cleared of prior convictions of identity theft through a background check prior to being allowed access. Access to administrative systems is granted to an individual based on the need to use specific data, as defined by job duties, and subject to the appropriate approval. A user's access cannot be shared, transferred, or delegated.

In cases where a parent seeks access to a student's records or in cases where an individual seeks access to a personnel file, the custodian of said records or his designee shall approve the access and verify the identity of the individual who wishes to view the files.

Securing Hard Copy Files

"Hard copy files" refers to files in printed format, both personnel records and student records. Every employee shall comply with the following instructions for securing hard copy files which contain NPI.

File cabinets, desk drawers, overhead cabinets, and any other storage unit containing documents with NPI must be kept locked. Desks, workstations, work areas, printers, and fax machines are to be cleared promptly of documents containing NPI. Employees are not to leave sensitive documents unattended on a fax machine, copy machine, or printer. Documents containing NPI must not be removed from LPSS premises or left in a vehicle.

Storage rooms containing documents with sensitive information and record retention areas must be kept locked, and access must be restricted to authorized personnel only. Each school principal or department director must maintain a key inventory for all rooms, filing cabinets, desks, and other storage units containing sensitive documents. Principals and supervisors must promptly secure the return of these keys from exiting personnel or from personnel who take extended leave from work. If an employee loses or misplaces a key, he or she must report the loss immediately to the supervisor who shall promptly have affected locks changed.

Securing Electronic Files

NPI stored on portable disks, hard drives, servers, microfilm, or by any other electronic means must be password-protected and accessible only to employees who must have access to this data in order to perform their daily jobs. Passwords should contain alpha, numeric, and other characters and should be changed on a regular basis. Employees are prohibited from sharing their passwords with others.

NPI should never be stored on laptop computers. Employees are prohibited from removing electronic files containing NPI from the LPSS premises. In the event that NPI must be transmitted to a third party service provider for processing or for reporting purposes, the data must be encrypted. Prior to contracting with a third party who will be handling NPI on behalf of the school district, the person responsible for overseeing the contract must receive clearance

from the Chief Information Officer, who shall verify the level of data security offered by the third party. Any contract with a third party who handles NPI on behalf of LPSS should address specific security requirements and the reporting of any breach in security. A service provider that maintains its own identity theft prevention program consistent with the guidance of the red flag rules and validated by due diligence may be considered as meeting security requirements.

Employees are required to maintain up-to-date anti-virus protection and anti-spyware on laptops owned by their respective schools or departments. LPSS's computer services division will be responsible for maintaining virus protection for all PCs that are part of the LPSS network.

When employees leave their desks, they must log off their computers to prevent unauthorized access to their desktop computers. When an employee separates from employment, the LPSS computer services division shall immediately terminate the separating employee's access to the LPSS network, including all access to e-mail, the student information system, the human resources information system, and/or the financial information system.

Use of Social Security Numbers

Employees' and students' social security numbers are not to be used as identification numbers except as required by financial institutions for tax purposes. The Human Resources Department, Payroll Department, and Insurance Department are the only areas of the organization which may require an employee's social security number on enrollment documents. All others are restricted to using the last four digits of the social security number on documents. This includes—but is not limited to--field trip forms for bus drivers, overtime reporting forms, substitute employee reporting forms, and stipend request forms.

Records Retention and Destruction

LPSS records shall be retained and destroyed as stated in the Record Retention Schedule maintained in the office of the Chief Financial Officer.

Discarded documents containing NPI must be shredded with a mechanical cross-cut shredder or a Department of Defense-approved shredding device. If paper documents cannot be shredded promptly, they should be placed in a locked shred bin for holding.

Supervisors who have a need to destroy electronic documents shall consult with the computer services division for instructions as to how the files should be deleted safely and thoroughly in order that they cannot be recovered by unauthorized persons. Computers which are retired and sent to auction should be wiped clean of all data, using "ghost-writing" software and not merely by deleting files.

Red Flags: Detection of System Failure

"Red flags" are signs that a security breach may have occurred which could result in unauthorized persons having accessed NPI. Red flags include such signs as

- Missing files or portions of files;

- Missing portable drives or disks;
- Stolen computers;
- Data deleted from or added to an electronic file which indicates someone who was unfamiliar with the data fields accessed a record; and
- Locks to an office or filing cabinet bearing evidence of tampering or forcible entry.

This is not an exhaustive list but is an illustration of the signs of a security breach. An employee who encounters a red flag should immediately report it to the Director of Risk Management.

Reporting and Responding To a Security Breach

In the event that the LPSS personnel discover a breach in security, the Director of Risk Management shall notify all individuals whose personal data has been, or is reasonably believed to have been, compromised. This notification shall also include tips on monitoring credit and accounts for identity theft and shall provide for the reporting of identity theft to LPSS and the proper authorities.

Identity Theft Prevention Program Administration

This policy providing for the security of information and data in the Lafayette Parish School System is adopted by the Lafayette Parish School Board for the protection of the identity of students and employees. Operational responsibility for the policy's maintenance is delegated to the Director of Risk Management, who shall serve as the district's compliance officer. The Chief Information Officer shall serve as an advisor to the compliance officer with respect to securing electronic documents.

All employees shall receive a copy of this policy upon its adoption, and new employees shall receive a copy of the policy when hired. Annual in-service meetings of employees must contain training regarding the protection of NPI and the reporting of any breach in security.

Enforcement of this Policy

Central office administrators and school-based administrators have the responsibility to implement and enforce this policy and to ensure that all employees and contractors follow it. LPSS employees are charged with safeguarding the integrity, accuracy, and confidentiality of NPI as part of the condition for employment. Any employee found to have violated this policy shall be subject to disciplinary action up to and including termination of employment in accordance with Policy File: GAEB:--Allegations of Misconduct. A violation of the policy may also result in the involvement of law enforcement agencies, when applicable.

Adopted: 1/19/00
Revised: 6/2/2010