# Transmitting Student Information Electronically

## Purpose

This data security segment is to help all Lexington City Schools staff members including Teachers, School Administrators, School Test Coordinators, Guidance Counselors, School Data Managers, Office Professionals, and Teacher Assistants to know how to securely transmit student information electronically. We must understand the legal and ethical responsibility to protect the confidentiality of student information and to use secure methods to carry out job responsibilities.

**Relevant Law:** FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records and applies to all schools that receive funds from the U.S. Department of Education.

Private information is referred to as Personally Identifiable Information (PII) in the education community. The term refers to information that can be used to distinguish or trace an individual's identity.

PII includes, but not limited to:

- Student's name
- Social Security Number
- Biometric records
- Name of student's parent or other family members
- Address of student or student's family
- State student number combined with other identifying information
- Other information that alone or in combination, linked or linkable to a specific student that would allow a reasonable person in the school community to identify the student

## Secure Methods of Transmitting PII Electronically

According to the *State of North Carolina Statewide Information Security Manual*, PII should be transmitted using across wireless or public networks either:

- Encrypted files
- Password protected files(as long as the password in not contained within the e-mail, file , or on the electronic device containing the data)

Secure FTP Servers

- emailed files only if encrypted and /or password protected using strong passwords(example mixed case and special characters)

**Non-Secure methods of Transmitting PII Electronically**

Non-secure methods of transmitting data electronically include any combination or data elements that allow individuals to be identified:

- fax
- email without encryption or password protection,
- sending IDs paired with any personally identifiable information
- listserv
- Google docs
- Dropbox

**Non-Electronic Methods Used to Communicate PII**

Although this segment is mainly about electronically transmitting student data, it is important to remember that non-electronic communication of student data is protected by FERPA. Any time we permit access to, release, transfer, or otherwise communicate, PII contained in education records to any party through oral, written, or electronic means we must protect student information.

Non-electronic means include the following;

- Student Rosters with PII posted to bulletin boards or announced on the intercom
- Student names and pictures with special programs identification without parent(s) approval or permission

- Student PII showing on unattended computer screen while an educator or staff is away from desk
- Discuss PII with anyone who does not have right or permission to obtain PII

Now that you know your responsibility for protecting student data, you can use acceptable methods mentioned above to transfer PII. The method of password protecting our files with student information attached to e-mails is an easy way to learn to protect student PII.

**How Do I Password Protect a Word/Excel Document?**

When the document or spreadsheet is completed, go to **File** and select **Save as**.

- Select drive and folder in which you wish to save the file, enter the name in the file box.
- Select **Tools** on the left of the **Save** button down at the bottom of the screen and select **General options**.
- You will be prompted to enter a password to open the file and then a different password to modify or change the file. You must type the To Open password again when prompted to proceed and then the To Modify password before you hit the **Save** button.
- **Close** the file and then Open the file to see if you have password protected the file.

If sending the file as an e-mail attachment, do not send the passwords in the same e-mail. It is best to communicate the passwords by telephone or to send in a separate e-mail that does not have the file attached.

These guidelines will help to ensure that we are protecting student PII and we are in compliance with federal law and state guidelines.