Handling and Transmitting Personally Identifiable Information

Local education agencies (LEAs), public schools, and NCDPI staff frequently need to share information from individual student records to resolve data issues and answer program area questions. Employees of LEAs, public schools, the NCDPI, or other education institutions are legally and ethically obliged to safeguard the confidentiality of any private information they access while performing official duties. Private information regarding students and staff should always be transmitted securely.

The FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that applies to all educational agencies and institutions (e.g., schools) that receive funding under any program administered by the U.S. Department of Education. Among several purposes, FERPA was enacted to protect the privacy of students' educational records.

For those LEAs and schools with full encryption capabilities, transported data and other electronic transporting devices containing NCDPI data should be encrypted. This requires the recipient of the data to have corresponding decryption capabilities.

To protect the confidentiality of individuals from those who are not authorized to have access to individual-level data, Personally Identifiable Information (PII) should be encrypted during transmission using one of the following methods, in order of preference:

- **Secure FTP** server based on SFTP or FTPS protocols.
    - Preferred method and most widely acceptable standard for transmitting encrypted data.
- **Encrypted Email**
    - If secure FTP capabilities do not exist, encrypted email can be used.
- **Password Protected Email**
    - If compatible encryption is not available to both parties, data should be password protected. The password should be given to the recipient through a different medium, such as a phone call, never in notes or documents accompanying the actual data file, or another email. In addition, the password should not be transferred via voicemail.

When sending e-mail, encrypted or password protected, please ensure that it contains the least amount of FERPA-protected information as possible. The subject line of an e-mail should not include FERPA-protected information; the body of an e-mail should not contain highly sensitive FERPA-protected information, such as a student's Social Security Number or full name. FERPA-protected data should always be in an attached encryted/password protected file, never in the body of an email.

Fax machines and printers used to send and receive secure data must be located in areas that are secure.

Secure test questions, answer choices, or portions of secure test questions or answer choices must not be sent via e-mail (use e-mail only if encrypted and/or password protected).

LEAs and schools should not use private or personal accounts to store students' personally identifiable information. LEAs and schools who wish to use the G suite for Education (previously called Google Apps for Education) should consult with their legal team to ensure compliance with FERPA and state security guidelines.
Furthermore, it is recommended that you use the Data Leak Protection (DLP) feature of G Suite to protect data, even though FERPA compliance does not require DLP.

For additional information, see the publication *Transmitting Private Information Electronically* the *Best Practices Guide for Communicating Personally Identifiable Information by E-mail, Fax, or Other Electronic Means*.