Data Management Group Policy

Electronic Transmission of Data

Policy Identification Number: DMG-2012-002-SE
Policy Name: Electronic Transmission of Data
Date Approved: August 30, 2012
Approval Authority: Data Management Group (DMG)
Statutory Reference: N/A

Policy Statement: The North Carolina Department of Public Instruction will protect the privacy of individuals in transmitting education data electronically.

Reason for Policy: To protect the confidentiality of individuals from those who do not have access to individual level data.

Policy Details: Secure Methods of transmitting data electronically include (but are not limited to) the following:

1) Encrypted Files,
2) Password Protected Files, (as long as the password is not contained within the email, file, or on the electronic device containing the data)
3) Secure FTP Servers, and
4) Emailed files only if encrypted and/or password protected

All sensitive mail attachments shall be sent either password-protected or via encrypted transmissions. For those business owners with full encryption capabilities, transported data and other electronic transporting devices containing DPI data should be encrypted. This requires the recipient of the data to have corresponding decryption capabilities. 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 separate e-mail or a phone call, never in notes or documents accompanying the actual data file. In addition, the password should not be transferred via voicemail.

The data should be secured in such a manner that it cannot be identified during the transportation process. The recipient's name, address, and telephone number should be clearly labeled in the body of the email message. While password protection is an adequate means for safeguarding transported data, it is a less desirable method and should only be used if encryption is not available.

Non-secure methods of transmitting data include any combination of data elements that allows individuals to be identified; fax; email without encryption or password protection; and sending IDs paired with any personally identifiable information. In addition, PII should not be shared in a Listserv, on Google Docs or through data-sharing services like Dropbox.

Related Documents: Reference DPI User ID and Password Protection Standards Policy:
https://intranet.ncpublicschools.gov/organization/technology-services/policies/DPI%20User%20ID%20and%20Password%20Standards%20Policy.pdf/view
Transmitting Private Information Electronically:
http://www.ncpublicschools.org/docs/data/management/best-practices.pdf

This policy applies to all data used by the agency in the performance of its mission. This data includes any that is collected, stored, processed, and/or disseminated using DPI information systems.
Version 2- 05/01/09

Contacts: The Division of Data, Research and Federal Policy is the proponent for this policy. Questions related to this policy or exception to the policy should be directed to the Enterprise Data Manager at 919-807-3241.

Revision History:

Version #	Version Date	Source file	Description of Change	Author