

# INTERNAL POLICY & PROCEDURE

---

## Topic Category:

Student Data Privacy

## Policy Title:

**Reporting, Exchanging, Storing, and Disposal of Personally Identifiable Information Policy**

## Purpose and Applicability:

All GaDOE employees, authorized representatives, and any other entity with access to student Personally Identifiable Information (PII) are responsible for protecting the data, which is also known as confidential data per GaDOE Information Classification Policy. Therefore, you must adhere to the following standard operating procedure and the GaDOE Acceptable Use policy also.

## Reporting Personally Identifiable Information

1. With the exclusion of standard public school enrollment reports, all public-facing reports or reports provided to non-authorized individuals that combine demographic and program participation information must adhere to the following rules:
  - If report is at district or school level, all cells' sizes less than 15 must be suppressed.
  - If report is of percentages, any percentage <5% or >95 % must be suppressed.
  - Totals for any column that has a suppressed value must also be suppressed.
  - Totals for any row that has a suppressed value must also be suppressed.Please note: The GaDOE Legal office may apply modified redaction rules to reports provided through Open Records Request.
2. Protect visibility of reports and computer monitors when displaying and working with confidential information.
3. If reports containing any individual student information are used in meetings or presentations, student names and date of birth must be masked.

## Storing Personally Identifiable Information

1. Please see Acceptable Use Policy section 1.6 on File Sharing and Data Storage
2. Store electronic data in a secure location only accessible by the authorized entity's approved individuals.
3. Do not store PII on DOE public "S" drive.
4. Paper documents containing PII must be kept in a secure location with limited access.
5. PII stored on portable devices must be secured by encryption with password.
6. Protect physical data (including hard copies of reports, storage media, notes, and backups) from unauthorized persons and secure when not in use.

## Exchanging Personally Identifiable Information

(Prior to exchange, confirm that the outside party understands this is PII and that they have the responsibility to secure it.)

1. Do not fax documents containing PII externally.
2. Do not email PII using the GaDOE official email system.
3. Use the MyGaDOE portal email system when emailing information containing PII to another user.
4. Use the agencies' Secure File Transfer Protocol (SFTP) system when sharing approved PII data with outside individuals or organizations.
5. Do not use personal email accounts to send PII.
6. Do not send PII data in Instant Messaging system.
7. Do not send PII data through social media.
8. Do not share files using cloud storage/sharing sites.

### Disposing of Personally Identifiable Information

1. Use shredders for hard copies
2. Permanently erase (not just delete) electronic records. Contact the GaDOE Information Technology department and submit a request for them to wipe the device that contained PII.
3. PII received via GaDOE official email system must be deleted immediately.

### Responding to Data Request for PII from Researchers

Request for PII data must be reviewed by the Data Privacy Review Board (DPRB) and either approved or denied.

- Approved PII data request will be forwarded to GaDOE's Legal Services Office for the creation of the Memorandum of Understanding (MOU).
- Approved PII data request will be entered into queue for processing after the MOU has been fully executed.
- All GaDOE MOUs involving the release of student-level identifiable data will be posted to the GaDOE website in compliance with Georgia's Student Data Privacy, Accessibility and Transparency Law. **See O.C.G.A. §20-2-664** by the Chief Privacy Officer.