



Duke University Graduate School Application Data Security Policy Revision Date: December 11, 2008

Purpose: The Admissions Office of the Graduate School recognizes that it handles, distributes, and transmits a great deal of sensitive information about student applicants to many administrative offices in departments and schools at Duke University. This information is covered under the Family Educational Rights and Privacy Act (FERPA) and is important to our operations and especially to the applicants involved. This policy will outline Graduate School expectations around handling of confidential information related to candidates for admission.

Policy: All Duke employees, including *but not limited to* Graduate School Admissions staff, Directors of Graduate Studies (DGS's), Admissions Committee members, DGS Assistants (DGSA's) and couriers who handle and administer Graduate School Admissions information are required to maintain the confidentiality and security of all applicant information. All Duke employees who handle Graduate School applications should become familiar with [FERPA](#) law.

DGS's are responsible for ensuring that the following 'best practices' and Graduate School policy regarding the handing of confidential data are adhered to:

- Transportation of Graduate School admissions files and loose documentation must be done in such a way that all student information remains secure and confidential.
- Current Graduate Students are not permitted to participate in the application process. This includes transportation of applicant information or otherwise handling or reviewing application packets.
- Application packets and other information related to applicants must be stored in a secure (i.e. lockable) location.
- All Duke employees who participate in the applications review process in any way, including *but not limited to*, transportation, administration and review, must have on file a signed copy of the [Duke University Confidentiality Agreement](#) and/or the [SISS Confidentiality Agreement](#).
- The Graduate School strongly discourages the practice of printing or creating electronic copies of application data material, however, recognizes that sometimes this is unavoidable due to the relatively short application season and the number of applications received.

- If applicant file materials are printed, the DGS is responsible for ensuring that all printed documents are returned to the DGSA (or designated departmental applications coordinator) and shredded after use.
- If a department chooses to make electronic copies of applications the electronic files must be individually password protected and encrypted in Adobe Acrobat, following the procedure outlined at oit.duke.edu/docprotection.htm
- The Duke University Blackboard is the only approved system to be used for distribution, review and commentary of application files by admissions committee members. Instructions for posting secure documents on the Blackboard are available on the OIT Web site at [Interim Secure Imaging Protocol](#).
- Only necessary documentation for admitted students should be kept for departmental files. (Note that all application documentation for admitted students will be available electronically.)
 - In order to maintain confidentiality, letters of recommendation may not be retained in a departmental copy of a student's file. All copies of letters of recommendation must be destroyed. Original letters of recommendation must be returned to the Graduate Admissions Office.
- Departments and programs will follow [Duke University Student Records Retention Guidelines](#).

Related Links:

[Family Educational Rights and Privacy Act](#)

[Duke University Confidentiality Agreement](#)

[PeopleSoft SISS Confidentiality Policy](#)

[Duke University Policy and Procedures under FERPA](#)

[OIT Interim Secure Imaging Protocol](#)

[Duke University Student Records Retention Guidelines](#)