Duke University Graduate School
Application Data Security Policy
Revision Date: September 2, 2014

Purpose: The Admissions Office of The Graduate School recognizes that it handles a great deal of sensitive information about student applicants and distributes and transmits that information to many administrative offices in departments and schools at Duke University. To the extent that some of the applicants will eventually matriculate, this information should be handled as if it were 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 (DGSs), Admissions Committee members, DGS assistants (DGSAs), and all others 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.

DGSs are responsible for ensuring that the following best practices and Graduate School policy regarding the handling of confidential data are adhered to:

- Current Graduate School students are not permitted to participate in the application process.
- All Duke employees who participate in the application 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.

- The Graduate School strongly discourages the practice of printing or creating electronic copies of application data material. However, it recognizes that on rare occasions, it is sometimes unavoidable due to the relatively short application season and the volume of applications received.

    If a department chooses to print applicant materials, the DGS is responsible for ensuring that all printed documents are destroyed after the admission decision has been made.

    - If a department chooses to make electronic copies of application materials, the electronic files must also be destroyed after the application review has been completed.
    - The DGS is responsible for conveying the Application Data Security Policy to members of the admissions committee(s).

- Only absolutely necessary documentation for admitted students should be kept for departmental files. The application, transcripts, and other supporting materials are stored in ImageNow and should not be maintained separately by the department.
- In order to maintain confidentiality, letters of recommendation in any form must not be retained in a departmental copy of a student's file. Once a student is matriculated, The Graduate School purges the letters of recommendation.
- The application dossier contains letters of recommendation and therefore should not be saved in departmental files.
- Rejected applicant files are kept on file in The Graduate School for a period of one year before being purged.
- Departments and programs will follow Duke University Student Records Retention Guidelines.
- Departments and programs will cooperate with the Graduate School Admissions Office and the SISS Office to update security rights every year.

Related Links:

Family Educational Rights and Privacy Act

Duke University Confidentiality Agreement

SISS Confidentiality Policy

Duke University Policy and Procedures under FERPA

Duke University Student Records Retention Guidelines