FLORIDA ATLANTIC UNIVERSITY

Office of the President
University Policy

SUBJECT:	**Effective Date:**	**Policy Number:**	
GENERAL PRIVACY POLICY	4-15-19	8.1	
	Supersedes:	**Page**	**Of**
	New	1	6
	Responsible Authority:		
	Chief Compliance & Ethics Officer		

APPLICABILITY:

This policy relates to the collection, use, and disclosure of all personal data provided by individuals to Florida Atlantic University ("FAU" or "University"). This policy applies to all areas of the University that may collect or process personal data from individuals.

DEFINITIONS:

Data Subject: A natural person whose personal data is submitted to the University with regard to certain activities while in the European Union, irrespective of that natural person's nationality or permanent place of residence. The personal data must be created in the European Union and transferred out of the European Union to the University.

Information: Includes any data concerning a natural person that is created by or provided to the University from or concerning applicants for enrollment or employment, prospective applicants, current students, former students, faculty and staff, donors, and research subjects.

Personal data: Any information relating to an identified or identifiable natural person, which is someone who can be directly or indirectly identified, including but not limited to a name, identification number, location data, physical address, email address, IP address, radio frequency identification tag, photograph, video, voice recording, biometric data (eye retina, fingerprint, etc.), or an online identifier of one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.

Sensitive information: Includes race, ethnic origin, religious or philosophical beliefs, trade union membership, health data, sexual orientation, and criminal convictions. Sensitive information may also include birthdates and personal identification information.

POLICY STATEMENT:

Florida Atlantic University is committed to safeguarding the privacy of personal data. The University does not collect personal information about an individual unless the individual chooses to make such information available to the University.

A. Collection and Use of Personal Data

Legitimate Interests. The University collects and processes information and sensitive information from individuals, including without limitation Data Subjects, only as necessary in the exercise of the University's legitimate interests, functions, and responsibilities as a public research higher education institution.

Research and Statistics. The University collects and processes information and sensitive information from individuals who are research subjects in the exercise of scientific, for historical research, or for statistical purposes, including without limitation general demographic and statistical research to improve University programs.

Employees. The University collects and processes information from employees, including individuals who are applicants for employment, to respond to their application and enter into or administer a contract or other employment relationship with the University. Upon receiving an applicant's consent, the University collects information concerning judicial measures and data to consider the applicant for employment and uses information, and data concerning an applicant or employee, to administer payroll and benefits, provide reasonable accommodations, and comply with applicable laws and regulations.

Students. Information is collected from students, including prospective students, and shared with internal and external parties to administer their application, register or enroll persons in the University, provide and administer housing, manage accounts, provide academic advising, develop and deliver education programs, administer academic record, administer athletics, provide support services, track academic progress, analyze and improve education programs, comply with University policy, recruit, compose regulatory reports, audit, maintain accreditation, and other related University processes and functions.

Reporting, Auditing and Accrediting. The University uses sensitive information concerning race and ethnic origin for regulatory reporting, auditing, and accrediting purposes. Sensitive information is collected, processed and shared internally and externally, as necessary, applicable and appropriate, to identify appropriate support services or activities, administer payroll and benefits, provide reasonable accommodations, enforce University policies or comply with applicable laws.

Contractual Relationships. Information and sensitive information may be shared by the University with third parties who have entered into contracts with the University to perform functions on behalf of the University, subject to the obligation of confidentiality and safeguarding from unauthorized disclosure.

Website Use: When an individual visits the University's website, the University's Web server automatically recognizes only the Internet domain and IP address from which the individual

accessed the University's website. This information does not result in the identification of the individual's personal e-mail address or other personal information. In addition, the University gathers information regarding the volume and timing of access to its website by collecting information on the date, time and website pages accessed by visitors to the website. The University does this so that it can improve the content of our website. Only aggregate information is collected, and individual personal information is not identified.

Online Payments. The University may collect credit card information for application fees, enrollment deposits or to process other University payments. A reputable third-party financial institution handles University credit card transactions. Whenever credit card information is transmitted through the University's website, the numbers and letters are scrambled using encryption technology to protect the information from being stolen or intercepted. For security purposes, the University does not allow individuals to store their credit card number from session to session.

Marketing. The University collects information and sensitive information provided by individuals in the marketing context in order to respond to their requests, offer services or programs, communicate with constituents about University programs, and personalize content of communications. The University maintains information about its constituents to analyze demographic and marketing information, to solicit potential constituents or donors, to recruit potential students, faculty, and staff, to research, analyze, and identify individuals interested in developing relationships or with existing relationships with the University, such as donors, friends, and alumni, to generate reports based on areas of interest, to review and evaluate University programs, as well as to manage prospective, current, or former participants of University programs. The University sends information about upcoming events, opportunities for giving back, and news regarding the various programs offered at the University by mail, phone, and email. The University will not send you these communications unless you opt-in to receive this information. This information will be used for alumni activities, including sending University publications, promotion of alumni benefits services, events, and programs. You have a right at any time to stop us from contacting you for marketing purposes at any time without detriment. If you no longer wish to be contacted for any of the above marketing purposes, please refer to Marketing Communication Opt-Out Request Form to opt out.

B. Sharing of Personal Data

Consent. The University may share sensitive information and other information when it has a person's consent.

Parents and Guardians. The University may share a student's information with a parent or guardian, consistent with University policy and regulations, and state and federal law.

Emergency Circumstances. The University may share information with third parties if, in the University's sole judgment, such disclosure is necessary to protect the health, safety, welfare, or property of any person. The University may share sensitive information and other information when necessary to protect a person's interests and safety or fulfilling health and wellness obligations established by law. Sensitive information regarding judicial measures will be processed only for purposes relating to a health or safety emergency and complying with any applicable provision of law.

Employment Necessity. The University may share sensitive information when necessary for administering employment or social security benefits in accordance with applicable law or any applicable collective bargaining agreement, subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

Charitable Organizations. The University may share information with the University Foundation and other University-affiliated not-for-profit organizations in connection with charitable giving, subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

Public Records. The University may share sensitive information and other information if a person has manifestly made it public or if otherwise required by State or Federal law, including Florida's public record laws. As an agency of the State of Florida, information shared with the University is subject to disclosure under the Florida Public Records laws, unless specifically exempted. If an individual chooses to share personal information with the University, it may be released if required by the Florida Public Records Laws or in accordance with our policies, rules or regulations and must be saved for a designated period of time to comply with Florida's record retention policies.

Archiving. The University may share information and sensitive information for archiving purposes in the public interest, and for historical research, and statistical purposes.

Performance of a Contract. The University may share information when necessary to administer a contract.

Legal Obligation. The University may share information when the disclosure is required or permitted by international, federal, and state laws and regulations, including the laws and regulations of the United States, the State of Florida, and the Florida Board of Governors.

Service Providers. The University may use third parties who have entered into a contract with the University to support the administration of University operations and policies. In such cases, the University may share information with such third parties subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

Counselors and Administrators. The University may use information and share it with counselors and administrators, consistent with University policy and regulations, and state and federal law.

Safety and Wellness Obligations. The University may share sensitive information relating to health conditions, food habits, and immunizations for the purpose of protecting University safety or fulfilling health, safety, and well-being obligations. Such information may be shared with University components as well as public and private third parties, including hospitals, clinics, public safety authorities, law enforcement, judicial bodies, security administrators, insurance companies, and other entities that are required by law to have such records.

University Affiliated Programs. The University may share information with parties that are affiliated with the University for the purpose of contacting individuals about goods, services, charitable giving or experiences that may be of interest.

De-Identified and Aggregate Information. The University may use and disclose information in de-identified or aggregate form without limitation.

Research and Studies. The University may share information with third parties that study admissions or other topics related to higher education. The University may also share information with third parties that conduct research or develop products or services designed to improve higher education functions. If the University shares information for this purpose, it will be de-identified. The University may share Sensitive Information with third parties to comply with a Legal Obligation or with appropriate consents.

Student Information. Consistent with the Family Educational Rights and Privacy Act of 1974 (FERPA), Florida statutes and University regulations, the University will not release personally identifiable information from education records without the written consent of the student. Exceptions to this rule include health or safety emergencies, educational authorities, school officials, parent(s) who claim the student as a dependent on the most recent year's federal tax return, and other exceptions as provided by law. Pursuant to the authority provided by FERPA, the University has designated certain information as "directory information" that the University may release upon request, or otherwise publish, unless specifically notified by the student in writing. The information designated as directory information is set forth in University Regulation 4.008.

C. Protecting Personal Data

The University implements appropriate technical and organizational security measures to protect information when it is transmitted and stored on the University's information technology systems. Applicants must have a secure browser—one that supports secure transmission of data across the Internet—to apply online to the University. No data transmission or storage can be guaranteed to be 100% secure. Application account passwords are protected so that only the applicant can access it and view the information that provided through the application portal. Passwords shall not be shared with anyone.

D. Retention and Destruction

Information will be retained by the University in accordance with the applicable retention periods in the Record Retention Schedule adopted by the State of Florida (General Records Schedule) and the Florida Board of Governors. Pursuant to Florida law and the General Records Schedule for Public Universities and Colleges, student education records will be retained permanently. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of information given the level of sensitivity, value and criticality to the University. Additional information about the retention and destructions of University records may be found in University Policy 5.2 Records Management.

E. Data Subjects

Data Subjects may request access to, a copy of, rectification, or restriction in the use of their information in accordance with all applicable laws, including without limitation Florida's public records law and records retention laws. If a Data Subject provided consent to the use of their information, they have the right to withdraw consent without affecting the lawfulness of the University's use of the information prior to receipt of their request. Data Subjects may email privacy@fau.edu with regards to a request noted herein. If a Data Subject feels the University has not complied with foreign laws regulating such information, a Data Subject may file a complaint with an appropriate supervisory authority in the European Union.

F. Updates

The University may, in its sole discretion, change, modify, add, remove, or other revise this policy at any time, consistent with the requirements of applicable law. Continued use of the University's website and third party applications after any such change indicates acceptance of and consent to these changes.

INITIATING AUTHORITY: Chief Compliance & Ethics Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 8.1

Initiating Authority
Signature: _____ Date: _____
Name: Elizabeth F. Rubin

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: Elizabeth F. Rubin

President
Signature: _____ Date: _____
Name: Dr. John Kelly

Executed signature pages are available in the Office of Compliance