



Jessup University Information Security & Privacy Notice

Jessup University ("Jessup") is committed to safeguarding privacy in the collection, processing, and sharing of personal data. Jessup collects and processes personal data ("Information") from individuals only as necessary in the exercise of the University's legitimate interests, functions, and responsibilities as a private, non-profit institution of higher education. This document describes the personal data we collect, process, and share; the measures we take to protect the privacy of that personal data; and the rights you have in connection with those activities. When information is submitted to the University, or you use the University's websites and other services, you consent to the collection, use, and disclosure of that information as described in this privacy notice.

This policy is designed to comply with the Gramm-Leach-Bliley Act (GLBA) and its Safeguards Rule, which requires financial institutions, including higher education institutions, to protect customer financial information.

Information We Collect and Process

Information collected from students or student applicants is used to register or enroll persons in the University, provide and administer housing to students, manage a student account, provide academic advising, develop and deliver education programs, track academic progress, analyze and improve education programs, recruitment, regulatory reporting, auditing, maintenance of accreditation, and other related University processes and functions.

The University also uses information to conduct general demographic and statistical research to improve University programs, to identify appropriate support services or activities, provide reasonable accommodations, enforce University policies, or comply with applicable laws. Information may be shared by Jessup 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.

We do not share nonpublic personal information with non-affiliates. Jessup stores the personal data it collects and processes what is essential for its operations. Nonpublic personal information (NPI) protected under GLBA includes, but is not limited to, financial aid records, student loan data, bank account/payment details, and tax records provided for financial aid purposes.

Lawful Grounds upon Which the University May Process Personal Data

The University may process your personal data on the grounds of contractual necessity, legal obligation, vital interests, public interest, legitimate institutional interests, or with your consent. NPI covered under GLBA is processed under contractual necessity, legal obligations, and legitimate institutional interests.

Third Party Use of Sensitive Information

We may disclose your Sensitive Information and other Information as follows:

- Consent, Emergency Circumstances, Employment Necessity, Public Information, Archiving, Performance of a Contract, Legal Obligation.
- Service Providers: We use third parties who have entered into a contract with the University to support the administration of University operations and policies. As required by GLBA, these contracts obligate service providers to implement and maintain appropriate safeguards consistent with Jessup's standards and federal law to protect nonpublic personal information.
- University-Affiliated Programs and De-Identified and Aggregate Information.

Retention of Your Information

Your information will be retained by the University in accordance with applicable state and federal laws.

Information Security

Jessup implements safeguards to:

- ensure the security and confidentiality of data, information (electronic and print), and resources;
- protect against anticipated threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of data, information, and resources.

The Jessup Information Security Plan describes precautions we take to prevent loss, misuse, or alteration of your personal data.

In accordance with GLBA, Jessup has designated the Information Security Officer as the GLBA Program Coordinator responsible for implementing and monitoring safeguards. All employees receive annual training on safeguarding practices. The University conducts periodic risk assessments to identify and evaluate risks to customer information and implements safeguards in line with GLBA requirements.

Transfers of Collected Information

We are located in the United States. By submitting your personal data via any Jessup web site or various servers and software systems, you transfer your personal data to us. Jessup and third-party data processors it contracts with operate secure data networks protected by industry standard firewall and password protection systems. Only authorized individuals have access to the information you provide. All security and privacy policies are periodically reviewed and enhanced as necessary.

Updates to This Policy

We review these privacy practices from time to time and these practices are, therefore, subject to change. We may update or change this policy at any time and users are asked to periodically review this policy to ensure continuing familiarity with the most current notice. As required by GLBA, Jessup University provides an annual privacy notice to students and others whose nonpublic personal information is collected for financial services. The notice is emailed to students at least annually, and the most current notice remains available on the consumer information page at Jessup.edu.