

FERPA and The General Data Protection Regulation (GDPR)

What is The Family Educational Rights and Privacy Act of 1974?

James Madison University adheres to and annually informs students of the Family Educational Rights and Privacy Act of 1974, as amended. This act, with which the university complies, was designated to protect the privacy of educational records. Under the Family Educational Rights and Privacy Act (FERPA) students have certain rights with respect to their education records.

These rights include:

1. The right to inspect and review the student's education records within 45 days of the day the University receives a request for access.
2. The right to request the amendment of the student's education records that the student believes are inaccurate or misleading.
3. The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.
4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by James Madison University to comply with the requirements of FERPA.

For more detailed information, refer to JMU Policy 2112: The Family Educational Rights and Privacy Act. [James Madison University, Policies and Procedures, Policy 2112, The Family Educational Rights and Privacy Act.](#)

What is the General Data Protection Regulation?

The [General Data Protection Regulation](#) is a [European Union \(EU\)](#) regulation designed to protect the privacy rights of individuals **located** in the [European Economic Area \(EEA\)](#). An individual need not be a citizen of a country in the EEA to be protected by the GDPR.

GDPR replaces prior EU privacy regulations and introduces broader protections than U.S. privacy laws such as HIPPA (Health Insurance Portability and Accountability Act) and FERPA (the Family Education Rights and Privacy Act).

How JMU Collects and Uses Personal Data

As an institution of higher education involved in education and research, JMU collects student data in many ways, including, but not limited to, the following: admissions applications, financial aid applications, enrollment transactions, grade submissions, and research initiatives.

In order for JMU to facilitate student enrollment in courses, issue grades, award degrees, and conduct other services related to enrollment and graduation, it must collect, use and process this personal data.

Lawful Basis for Data Processing under the GDPR

James Madison University processes personal data of individuals located in the European Economic Area (EEA) in accordance with the General Data Protection Regulation (GDPR). The lawful bases for processing such data may include:

- **Consent** – when the individual has freely given clear and informed permission for their data to be processed for a specific purpose.
- **Contractual Necessity** – when processing is necessary to fulfill a contract with the data subject, such as enrollment, course participation, or employment.
- **Legal Obligation** – when processing is required to comply with applicable laws or regulations.
- **Legitimate Interests** – when processing is necessary for the university's legitimate educational, research, or administrative interests, provided such interests are not overridden by the data subject's rights and freedoms.
- **Vital Interests** – when processing is necessary to protect someone's life or health.
- **Public Task** – when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

JMU ensures that personal data collected in or transferred from the EEA is handled with appropriate safeguards and in compliance with GDPR requirements. Individuals whose data is subject to GDPR have rights regarding access, correction, deletion, and objection to processing, which JMU respects and facilitates.

How Does JMU Protect Collected Data?

Data Stewardship and Information Security Framework

The Data Stewardship and Information Security Framework guides JMU's management and protection of University Data in accordance with university policies as well as applicable laws, regulations, and contractual obligations. The Framework is based on the policies, standards, and procedures that outline the roles and responsibilities of key stakeholders, the classification of data and systems, and a strategy for continual assessment of data stewardship.

As stated in University Policy 1205 – Data Stewardship, University Data is defined as data collected, maintained, or used by university personnel, contractors, or partners as part of their job responsibilities, for operation of the University or to fulfill its mission. University Data may be represented in a variety of data elements, types, and forms maintained by individuals, administrative/academic units, or business partners to provide functionality to the University. All such data is considered University Data unless explicitly excluded in writing.

How Long Does JMU Retain Collected Data?

JMU maintains a university records management program according to Commonwealth of Virginia law and internal policies. See JMU policies 1109 (Records Management) and 3015 (Records Retention and Disposition) for more information.

Protected Data under FERPA and the GDPR

What are education records according to FERPA?

Under FERPA, education records are defined as records that are directly related to a student and are maintained by an education agency or institution or by a party acting for the agency or institution. Education records can exist in any medium, including: typed, computer generated, videotape, audiotape, film, microfilm, microfiche and email, among others. These records may not be disclosed without student consent or by satisfying one of the FERPA exceptions.

How does a student provide consent to disclose education records under FERPA?

Students may complete the Declaration of Dependent Status form (<https://www.jmu.edu/registrar/ferpaoutline.shtml>) to authorize JMU to disclose education records to those individuals they list on the form. JMU will disclose records upon written request and verification of dependency or consent.

What is Personal Data under the GDPR?

Personal data collected in, or transferred from, any of the applicable countries in the EEA is subject to the GDPR. Under the GDPR, “personal data” refers to any information that relates to an identified or identifiable natural person (i.e., an individual, not a company or other legal entity), otherwise known as a “data subject.” Examples of “personal data” include a person’s name, email address, government-issued identification, or other unique identifier such as an IP address or cookie number, and personal characteristics, including photographs.

The GDPR highlights some “special categories” of personal data, which merit a higher level of protection due to their sensitive nature and consequent risk for greater privacy harm. This includes information about a data subject’s health, genetics, race or ethnic origin, biometrics for identification purposes, sex life or sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership. Although criminal convictions and records are not considered “special categories” of personal data, this information is subject to amplified protections under the GDPR.

In the circumstances referenced above, JMU considers the personal data that is collected in, or transferred from, any of the applicable EEA members to be protected data, and not disclosable without student consent.

How does a student provide consent under the GDPR?

If personal data is being collected in, or transferred from, any of the EEA members, JMU must secure student consent to disclose that information. GDPR stipulates that consent must be freely given, specific, informed and an unambiguous indication that the Data Subject has consented to the particular Processing of Personal Data. Consent form (In Development).

What is Directory Information according to JMU?

The following is considered "Directory Information" at James Madison University and may be made available to the general public unless the student notifies the Office of the Registrar in person or in writing within five days after the first day of class registration:

- Student's name,
- Degree sought and time,
- Major/minor fields of study,
- College of major and year (freshman, sophomore, etc.),
- Enrollment status (full-time/part-time) including credit hours,
- Dates of attendance,
- Degrees, awards and honors conferred,
- Participation in officially recognized activities and sports,
- Weight and height of members of athletic teams,
- The most recent previous educational agency or institution attended by the student,
- Fraternity and/or sorority and educational societies.

Enrolled students may "opt in" to three additional data elements of directory information: address, email address, and telephone number.

Note: Personal data collected in or transferred from EEA member countries may be subject to GDPR protections, even if it qualifies as Directory Information under U.S. law.

What if I have questions?

If you have specific questions regarding the collection and use of your education records and/or personal data as governed by the GDPR, please contact the Office of the Registrar at registrar@jmu.edu.