

EEA General Data Protection Regulation Privacy Notice - University of Rochester Prospective and Admitted Students Located in the EEA

This Notice describes the practices of the University of Rochester (the “University”) with respect to the collection, use, storage, and disclosure of Personal Data covered by the European Union’s General Data Protection Regulation relating to prospective and admitted students who are located in the European Union and the European Economic Area (the “EEA”) in the context of the University’s admissions and financial aid activities. This Notice applies only to the use of Personal Data in EEA Processing Activities. When you submit your application to the University, or otherwise provide the University with information in connection with your admission or enrollment with the University, you consent to the University’s collection, use, processing and disclosure of that information as described in this Notice.

In this policy,

- “**GDPR**” means the European Union’s General Data Protection Regulation;
- “**Personal Data**” means information that relates to an individual who is directly or indirectly identified or identifiable; and
- “**EEA Processing Activities**” means the collection, use, processing or sharing of Personal Data when those activities are within the scope of the GDPR.

In this Notice the words “we”, “us” or “our” refer to the University of Rochester, and the word “you” or “your” refers to prospective and admitted students and their families.

Personal Data We Collect

We collect, store, and process a variety of Personal Data as part of our admissions and financial aid processes. For example, the University collects the following categories of Personal Data in the context of its admissions and financial aid activities:

- Contact Information – Your name, home and alternate addresses, email address and phone number;
- Demographic Information – Your birth date, birthplace, race, ethnicity, citizenship status and gender;
- Education History – Your prior schools, transcripts, honors, school activities and disciplinary records;
- Testing History – Your standardized testing information;
- Personal Information and History – Your personal interests, extracurricular activities, recommendations, and other information we may learn about your personal background;
- Employment History – Your job title, location and work experience;
- Personal Financial Information – Your government identification number, personal and business tax reports, wage reports and statements, bank statements, socioeconomic status, scholarships and grants, and family support;

- Family Information – Your family member names, birthplaces, email addresses, phone numbers, ages, education information, occupations, wages and savings, and marital status;
- Immigration Information – Your information related to visa requirements and copies of passports;
- Criminal Record History – Your criminal record, including self-reported information and information available in the public record; and
- Payment Information – Your payment card number or your bank and bank account number, depending on your means of payment.

How We Collect Personal Data

The primary source of Personal Data collected is your application to the University. In addition to submitting an application directly to us, you may submit an application through the Common Application or via other third party sites through which the University collects prospective student information or financial aid related data. During the recruiting and application process, you may also provide us with Personal Data through other means, including through communications with University employees or by completing a “prospect” card. In addition, we collect contact, academic and demographic information from third parties who provide us information about prospective students who may be interested in attending the University.

Purposes and Legal Basis for Processing Personal Data

The Personal Data we collect, or that is collected on our behalf, during the admissions process is collected for the primary purposes of considering your candidacy for admission to the relevant University school, program or course, evaluating your eligibility for financial aid, if applicable, and, if you are admitted and enroll, facilitating your education. If you are admitted and enroll to the University, we will share such Personal Data with registrars and other University departments in order to enable your enrollment and participation in the school, program or course to which you have been admitted, and to otherwise facilitate your education. For example, certain Personal Data may be shared with a professor in whose course you enroll, in order to administer financial aid, to track your progress at the University, in order to accommodate your disability, to enable you to obtain treatment with University Health Service (UHS), or for other reasons consistent with our efforts to provide educational services to you. We will also provide certain Personal Data, such as contact information, demographic information, education information and family history to the University Office of Alumni Relations.

The University’s lawful bases for processing your Personal Data include the following: (i) the University’s legitimate interests, (ii) to carry out our responsibilities under a contract, to process transactions requested by you or in order to take steps at your request prior to entering into a transaction or contract, (iii) to comply with laws applicable in the European Union or its member states, or (iv) your consent, where applicable. With respect to item (i) above, we have a legitimate interest in recruiting, admitting and enrolling qualified applicants, in providing

student financial support and administering financial aid programs, in facilitating the provision of educational services and in complying with laws and regulations that govern our conduct in the countries where we operate.

How We Share Personal Data

Your Personal Data will be received and processed by University representatives in connection with the purposes of processing described above. We may share your Personal Data among University divisions, programs and initiatives as described above. We may also share the information with service providers we have retained to perform services on our behalf, such as to the provider of our student information CRM system and to organizations who provide research insights using our admissions and financial aid data. We share your Personal Data with such service providers only when they have agreed to process your Personal Data only to provide services to us and have agreed to protect your Personal Data from unauthorized use, access, or disclosure. We may also make certain “directory information” publicly available in accordance with our Family Educational Rights and Privacy Act (FERPA) policies and procedures.

We may also disclose your Personal Data to legal or government regulatory authorities as required by applicable law. We also disclose your Personal Data to third parties as required by applicable law in connection with claims, disputes or litigation, when otherwise required by applicable law, or if we determine its disclosure is necessary to protect the health, safety, rights or property of you, us or others, or to enforce our legal rights or contractual commitments that you have made.

How We Protect Your Data

The University uses risk-assessed administrative, technical, and physical security measures to protect against unauthorized use, disclosure, alteration, or destruction of the personally-identifiable information we collect. Only authenticated users with specific permissions may access the data. We encrypt your data in transit using secure TLS cryptographic protocols. We use network segmentation and monitoring to evaluate any attempts at accessing the systems without permission. We maintain a documented vulnerability management program which includes periodic scan, identification, and remediation of security vulnerabilities. Critical patches are applied to servers and workstations on a priority basis. We also conduct regular internal and external penetration tests and remediate according to severity for any results found. All University Information Security Policies and Procedures are based upon current industry best practices and common security frameworks.

Your Rights

You have certain rights regarding your Personal Data, subject to certain exclusions as described in the GDPR. This Notice summarizes what these rights under the GDPR involve and how you can exercise these rights. More detail about each right, including exceptions and limitations, can be found in the applicable text of the GDPR.

- Right of Access – You have the right to request that the University confirm whether it is processing your Personal Data. If the University is processing your Personal Data, you have the right to access that Personal Data, and the University will provide you with a copy of that Personal Data unless prevented by applicable law;
- Right of Rectification – You have the right to request that the University correct any inaccurate Personal Data that it maintains about you;
- Right of Erasure – You have the right to request the erasure of Personal Data that the University maintains about you in certain circumstances;
- Right to Restrict Processing – You have the right to request that the University restrict the processing of your Personal Data where one of the reasons identified in the GDPR apply;
- Right to Data Portability – In certain situations, you have the right to request a copy of your Personal Data in electronic format so that you can transmit the data to third parties, or to request that the University directly transfer your Personal Data to one or more third parties;
- Right to Object to Processing – In certain situations, you may have the right to object to processing of your Personal Data;
- Right to File Complaint – You have the right to file a complaint with your applicable European Union supervisory authority if you believe that the University’s processing of your Personal Data violates the GDPR.

In addition, if the basis for processing your Personal Data is consent, you may revoke your consent at any time. Note that, in certain cases, we may continue to process your Personal Data after you have withdrawn consent and requested that we delete your Personal Data, if we have a legal basis to do so.

Data Retention

The GDPR requires that your Personal Data be kept no longer than necessary. The applicable time period will depend on the nature of such personal data and will also be determined by legal requirements imposed under applicable laws and regulations. The University’s current Policy on Retention of University Records is available here: <https://www.rochester.edu/adminfinance/records.html>.

International Data Transfers

Personal Data that you provide while in the EEA will generally be transferred to the United States. If your Personal Data was collected or stored in the EEA, we may transfer your Personal Data outside the EEA and when we do so, we rely on appropriate or suitable safeguards recognized under data protection laws. The European Commission has adopted standard data protection clauses, which provide safeguards for personal information transferred outside of the EEA. We may use Standard Contractual Clauses when transferring Personal Data from a country in the EEA to a country outside the EEA. Where applicable, you can request a copy of our Standard Contractual Clauses by contacting us as set forth in the Contact Information section below. We may transfer your Personal Data from a country in the EEA to a country outside the EEA after having obtained your explicit and informed consent. We may also

transfer your Personal Data outside the EEA if (i) the transfer is necessary to the performance of a contract between you and the University, or if the transfer is necessary to the performance of a contract between the University and a third party, and the contract was entered into in your interest, or (ii) the transfer is necessary in order to protect your vital interests or of other persons, where you are physically or legally incapable of giving consent.

Policy Updates

We may change this Notice from time to time. We will publish on our website any changes we make to this Notice and notify you by other communication channels where appropriate.

Contact Information

If you have any questions, comments, requests or concerns about this Notice, you may contact Michael Sauter, Senior Information Analyst, Office of College Enrollment, at msauter@admissions.rochester.edu or 585-275-4689.