



# UNDERGRADUATE ADMISSIONS PRIVACY STATEMENT

## Overview

This Privacy Statement outlines the Undergraduate Admissions Department's collection, use, and disclosure of information provided by prospective students and applicants. When you provide information on your application for admission, register for campus events, or use our websites and other services, you consent to our collection, use, and disclosure of that information as described in this Privacy Statement.

## What information do we collect?

In order for Winthrop to recruit prospective students, review and process applications for admissions, and provide necessary information for enrollment and connection to the Winthrop community, it may collect the following personal information:

- Name
- Contact information including, without limitation, email address, physical address, phone number, and other location data
- Unique personal identifies and biographical information (e.g. date of birth, social security numbers, race and ethnicity)
- Details of your educational history
- Information related to visa requirements, copies of passports, and other documents to ensure compliance with U.S. laws
- Information related to both student and family members current employment status, driver's license information, vehicle registrations, and federal and state tax information to confirm South Carolina residency in compliance with S.C. laws

Information about your computer hardware and software is automatically collected by Winthrop University. This information can include: your IP address, browser type, domain names, access times, and referring website addresses. Winthrop uses this information to enhance your user experience and to provide general statistics regarding use of the Winthrop University website. You can set your browser to not accept cookies if you prefer.

## How do we use your information?

The information collected from prospective students and applicants is provided with their consent and shared with internal and external parties for outreach efforts, to improve our admissions process, to evaluate whether an applicant is suitable for admission to the University, and other related University processes and functions. The University also uses this information to conduct general demographic and statistical research. If you are accepted for admission to the University, we will use and share your information internally with other University offices as necessary and appropriate to support your success as a student, to deliver education, advising, residence, student development, financial aid, and to communicate the University's activities.

## How do we protect your information?

We seek to implement appropriate security measures to protect your information when you transmit it to us and when we store it on our systems. When using our online application, all data is received and transmitted over TLS, using 2048-bit keys. All data is stored in encrypted databases on encrypted file systems in secure datacenters, using 256-bit AES encryption.

Your application account password is protected so that only you can access it and view the information that you provide to us through your application portal. We strongly advise you not to share your password with anyone.

Student data is protected by the Family Educational Rights and Privacy Act of 1974 (FERPA). With few exceptions, the University cannot disclose any non-directory student information to anyone other than the student unless the student has given specific written consent. Admissions staff members receive training on FERPA rights and practices. Staff are also trained to follow the privacy and confidentiality policies outlined in this statement.

## Can information be corrected?

Our office works closely with all students regarding appropriate data entries. If you have any questions, or objections regarding the validity of your data, please contact our office as soon as possible if you believe there is an issue. In some instances, information has been obtained by an outside source. If information from these sources is incorrect, we will direct you to the source of the data to correct any inaccurate data.

## Information shared with outside parties

As a prospective student or applicant, we may also disclose your information to outside parties as follows:

- **Parents and Guardians:** In some cases, we may share your information with a parent or guardian if necessary to properly complete the admissions process or in the event of an emergency.
- **Service Providers:** We may use third parties to support our operations. In such cases, we may share your information with such third parties who are obligated to keep it confidential and safeguard it from unauthorized disclosure.
- **School Counselors and Administrators:** We may use your information and share it with your school counselors and administrators.
- **Research and Studies:** We may share your information with third parties that study admissions or other topics related to higher education. We may also share your information with third parties that conduct research or develop products or services designed to improve admissions and other higher education functions. If we do share your information for this purpose, it will be de-identified.
- **Required by Law:** We may share your information with third parties to the extent we are required to do so by law, court order, or subpoena.

## Third party links

Occasionally, at our discretion, we may include links to third party sites on our website (including, but not limited to, Facebook, Instagram, Twitter, YouTube, YouVisit, and others). Please be aware that we have no control, responsibility, or liability for the content and activities of these linked sites. These third party sites have separate and independent privacy statements and we encourage our users to be informed and aware and to read the privacy statements of any other site that collects your personal information. However, we continually seek to protect the integrity of our site and welcome any comments for improvements, including any links to third party sites.

## Compliance with the other jurisdictional privacy regulations

Other states or countries may have privacy regulations which serve to protect their citizens. For example, the European Union General Data Protection Regulation (GDPR) is a European Union (EU) legal framework for data privacy and security of personal data for individuals within the EU. The GDPR sets forth obligations for organizations that collect, use, share, and store personal data of constituents who reside in the European Union.

For prospective students located in the European Union, you may also have additional rights with respect to your information, such as: (i) data access and portability; (ii) data correction (including the ability to update your personal data); (iii) data deletion (including the right to have Winthrop University delete your personal information, except information we are required to retain, by contacting us); and (iv) withdrawal of consent or objection to processing (including, in limited circumstances, the right to ask Winthrop University to stop processing your personal data, with some exceptions, by contacting us). You may also be able to file a complaint with the appropriate supervisory authority in the European Union.

Students, or prospective students have created a contractual need with Winthrop University to collect and retain certain data at the time of submitting an application for enrollment. Personal information is required by the University as an essential part of the academic process and must be retained per legal requirements.

For non-students, Winthrop University is committed to securing the appropriate consent (opt-in) in the collection and processing of personal data. If you have any questions, or objections to the collection, use and retention of your personal data, on legitimate grounds, Winthrop University shall consider all requirements of notice, choice, transfer, security, data integrity, and access. Please direct any questions you may have concerning Winthrop University's obligations and compliance with GDPR to [privacy@winthrop.edu](mailto:privacy@winthrop.edu).

## How long do we keep your information?

Personal data will be retained in this office in accordance with applicable federal and state laws, regulations, and accreditation guidelines, as well as University policies. Personal data will be destroyed when no longer required for University services and programs, upon request or after the expiration of any applicable retention period, whichever is later. GDPR, or other jurisdictional privacy regulations, do not supersede legal requirements that Admissions maintain certain data.

## Your Consent

Student Data:

By enrolling in Winthrop University you have created a contractual need that requires the sharing of required personal information. Your consent was established at the time of enrollment.

By giving us your information via email, phone, fax, website, or other communication methods, you consent to our Privacy Statement.

## Changes to this Privacy Statement and University Policy.

Any changes to this policy will be posted to this website and the date noted at the bottom. Winthrop University policies, including our [University Privacy Policy](#), may be found in the Winthrop University [Policy Repository](#).

**Last updated: January 9, 2019**

## Contact Information:

If you have any questions regarding this statement please contact:

Winthrop University Office of Admissions at [admissions@winthrop.edu](mailto:admissions@winthrop.edu).