CONTROLLER'S OFFICE
PRIVACY STATEMENT

Overview

The Controller's Office provides accounting and business services for the instructional, research, and administrative components of the University. The Controller's Office is responsible for providing processes, systems, and controls over financial functions so that the University has timely, accurate, and complete financial information for use in decision making. The Controller's Office is also responsible for the preparation of the University's annual financial statements.

What information do we collect?

In the course of performing our services to our users, the Controller's Office collects banking information from our suppliers and other non-payroll vendors.

How do we use your information?

We use this information to electronically transfer payments to vendors both domestic and international.

How do we protect your information?

We use appropriate safeguards consistent with prevailing industry standards and commensurate with the sensitivity of the data collected to maintain security and integrity of that information in our systems and in our physical facilities. We utilize a variety of security measures, including locked storage, approved access to data, shredding of all hard documents not required to be retained, and password protection of electronic documents.

Can information be corrected?

We utilize the data collected by other departments such as Admissions, Student Financial Services, Financial Aid, Procurement, Human Resources and Payroll to perform our required job functions. We are always glad to assist with any questions or concerns. Our hours and contact information are posted on the Winthrop University website.

Information shared with outside parties

Information may be shared with third parties who assist us in providing services related to Winthrop vendor, student and faculty/staff accounts including (but not limited to):

- Banking Institutions (Deposits, direct deposits, payments, and wire transfers)
- Various State Treasurer's Offices (Escheated Property)
- Federal and State Authorities (Tax returns and other informational reporting requirements)
- Whenever we believe release is appropriate to comply with the law, enforce our site policies, or protect ours and other's rights, property, or safety.

Third party links

Occasionally, at our discretion, we may include links to third party sites on The Controller's Office website. The University is not responsible for the contents of any linked site, and you must adhere to the privacy policy of that site.

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.

We comply with all federal, state, and foreign privacy regulations. We also adhere to all federal, state and foreign authorities reporting requirements.

Students, or potential 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.

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 jurisdiction privacy regulations, do not supersede legal requirements that the Controller's Office maintain certain data.

Changes to this Privacy Statement and University Policy.

This policy may be revised from time to time due to legislative changes, changes, in technology, our privacy practices, or new uses of employee information not previously disclosed in this statements. Revisions are effective upon posting. Please refer to this policy regularly.

Last updated: August 20, 2019

Contact Information:

If you have any questions regarding this statement please find our contact information at the Controller's Office website.