# AP 3800 Personal Data Protection

**References: None**

The Chief Information Officer directs that the following regulations and procedures apply to all Rogue Community College students, faculty, staff, administrators, consultants, authorized guests, and any other persons granted access to College information resources. This group shall be referred to as “users.” The College is responsible for ensuring these procedures are readily accessible prior to use of any College systems or data.

These procedures apply to all systems, records, and processes that collect, store, process, transmit, or dispose of personal data in any form. This includes all electronic systems, paper records, cloud services, third-party systems, and devices connected to or interacting with the College Network. Hereinafter, all such systems and data shall be referred to as the “College Data Environment.”

**Personal Data Definition**

Personal Data is any information that identifies or can reasonably be used to identify an individual. This includes, but is not limited to:

- Name, address, phone number, and email
- Social Security Numbers and government-issued identifiers
- Student records protected under FERPA
- Financial and payment information
- Employee and personnel records
- Health-related information
- User credentials and authentication data

Certain data elements require a higher level of protection due to regulatory, legal, or operational risk. These are considered Sensitive Personal Data.

**Legal and Regulatory Requirements**

The handling of Personal Data must comply with all applicable federal and state laws, including but not limited to FERPA, Gramm Leach Bliley Act (**Gramm-Leach-Bliley Act (GLBA):** A federal law enacted in 1999 that requires financial institutions, including

colleges and universities that process student financial aid and other financial data, to protect the privacy and security of consumers' nonpublic personal information (NPI). GLBA includes the Safeguards Rule, which mandates the implementation of administrative, technical, and physical controls to ensure the confidentiality and integrity of this information.), Oregon Public Records Law, and Oregon data protection statutes.

Improper handling, disclosure, or misuse of Personal Data may result in disciplinary action, civil liability, and/or criminal penalties.

**Ownership and Accountability**

All Personal Data within the College Data Environment is the property of Rogue Community College. Access to data does not imply ownership.

Accountability is defined as follows:

- **Data Owners** determine how data is classified and who may access it
- **Data Stewards** ensure data is properly handled and maintained
- **Users** are responsible for protecting the data they access

There is no scenario where Personal Data is "unowned" or unmanaged.

**Data Classification and Handling**

Personal Data must be classified based on risk and sensitivity. At a minimum:

- Public
- Internal
- Confidential
- Restricted (Sensitive Personal Data)

Users are expected to know the classification of the data they handle and apply appropriate safeguards. When in doubt, treat data at the higher classification level.

**Collection and Use**

Personal Data will only be collected when it is necessary to support legitimate College operations.

Data collection must be:

- Purpose-driven
- Limited to what is required

- Accurate and maintained

Use of Personal Data must remain within the scope for which it was collected. Expanding use beyond that scope without authorization is prohibited.

**Access Control**

Access to Personal Data is not a convenience—it is a controlled privilege.

Access will be:

- Granted based on business need
- Approved by the appropriate authority
- Reviewed on a regular basis

Unauthorized access, even if no harm is intended, is a violation of this procedure.

**Data Protection**

Users are expected to actively protect Personal Data. At a minimum:

- Use strong authentication practices
- Do not share credentials
- Store data only in approved systems
- Encrypt data when required
- Secure physical records appropriately

Personal Data will not be stored on personal devices, unauthorized systems, or unapproved cloud platforms.

**Transmission and Sharing**

Before sharing Personal Data, users must:

- Confirm the recipient is authorized
- Use approved secure transmission methods
- Ensure appropriate agreements are in place for third parties

Sending Personal Data to the wrong recipient is a reportable incident.

**Retention and Disposal**

Personal Data will not be kept indefinitely.

Data must be:

- Retained only as long as required
- Disposed of securely when no longer needed

This includes proper deletion of electronic data and destruction of physical records.

**Incident Reporting**

If Personal Data is lost, exposed, or accessed without authorization, it must be reported immediately.

There is no “wait and see” period.

The College will investigate all incidents and take appropriate action, including required notifications under law.

**User Responsibilities**

Users are expected to operate with discipline and awareness when handling Personal Data.

This includes:

- Protecting data at all times
- Following all policies and procedures
- Completing required training
- Reporting issues immediately

Failure to do so will result in disciplinary action, up to and including termination or expulsion.

**College Rights**

The College reserves the right to monitor, audit, and access systems and data to:

- Ensure compliance
- Protect system integrity
- Meet legal and regulatory obligations

This is not optional and does not require prior notice when acting to protect the institution.

**Disclosure and Public Records**

Users must understand that certain data may be subject to disclosure under Oregon Public Records Law unless exempted.

The College will balance transparency with privacy, but users should not assume electronic data is private by default.

**Third-Party Requirements**

Vendors and third parties handling Personal Data must meet the College's security and data protection requirements.

This includes:

- Contractual agreements
- Appropriate safeguards
- Ongoing accountability

The College reserves the right to assess compliance at any time.

**Acknowledgement**

Use of College systems constitutes acceptance of this procedure.

Users will be required to acknowledge that they:

- Understand their responsibilities
- Will comply with all requirements
- Accept the consequences of non-compliance

**Rescinds Procedure Number: None.**

**Approved: May 12, 2026**