Applies to: *Faculty (including part-time and visiting faculty), staff and students (including graduate/undergraduate student workers and graduate assistants) employed by the University This policy continues to apply to individuals on sabbatical, other leaves or while visiting other institutions*

1. Guidelines:

Issued: June 2025
Last Revised:
Last Reviewed:

2. Purpose:

A practical guide to understand PII (Personally Identifiable Information)

3. What is PII:

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity—either alone or when combined with other personal or identifying data.

Common Examples of PII:

- Full name (especially when combined with other data)
- Social Security Number (SSN)
- Student or employee ID numbers
- Home or mailing address
- Personal phone numbers
- Email addresses linked to identity
- Date and place of birth
- Passport or driver's license numbers
- Biometric data (e.g., fingerprints, facial recognition)
- Financial account numbers

4. Why Protecting PII Matters

Legal Compliance: Universities must comply with laws like:
- FERPA (Family Educational Rights and Privacy Act) – protects student education records.
- HIPAA (Health Insurance Portability and Accountability Act) – protects health information.

Institutional Trust: Mishandling PII can damage the university's reputation.
Risk Mitigation: Data breaches can lead to identity theft, financial loss, and legal consequences.

5. Best Practices for Handling PII

Collect and Store Responsibly

- Only collect PII when absolutely necessary.
- Store PII in university-approved, secure systems (e.g., encrypted drives, secure cloud platforms).
- Avoid storing PII on personal devices or unencrypted USB drives.

Limit Access

- Share PII only with individuals who are authorized and have a legitimate need to know.
- Use role-based access controls where possible.

Communicate Securely

- Never send PII via unencrypted email.
- Use secure file transfer tools or encrypted email services approved by the university.

Dispose Properly

- Shred physical documents containing PII.
- Use secure deletion methods for digital files.

6. Reporting a PII Incident

If you suspect that PII has been lost, stolen, or improperly accessed:

Take Immediate Action:

1. Do not attempt to fix the issue alone.
2. Report the incident immediately to your university's IT Security Office or Data Protection Officer.

Include in Your Report:

- What type of PII was involved
- How the incident occurred (if known)
- When and where it happened
- Any individuals or systems affected

Why Reporting Matters:

Prompt reporting allows the university to:

- Contain the breach
- Notify affected individuals (if necessary)
- Comply with legal obligations
- Prevent future incidents

7. Responsibilities:

Position or Office	Responsibilities
Information Technology, CIO	Owns the policy and compliance procedures.

Data Owners	Enforce the policy

8. Related Information:

Related Policies
Information Security Policy
Data Governance Policy
Privacy Policy

9. Contacts:

Division/ Department	**Position or Office**	**Contact Information**
Information Technology	CIO	603-897-8630 / itsupport@rivier.edu