Information Technology

Privacy Policy

Version: 1.0 Date: 03/02/2021

Policy Title: Information Technology Resources Privacy Policy

Policy Type: Update to Existing Policy

Applicability: College-wide

Submitted By: Don Schattle/Dylan Bukaweski, Information Security Office (infosec@providence.edu)

Oversight Department(s): Information Technology

Effective Date: 04/06/2021

1. Policy Statement

Providence College owns and maintains various types of data, information, and records for the purpose of supporting its mission, goals, and values. Interaction with College data, especially that which is non-public in nature, must be treated as a highly sensitive task in order to safeguard the privacy of sensitive and proprietary information, and to ensure compliance with various legal and regulatory requirements.

Maintaining confidentiality and privacy is a community-wide effort involving the support and participation of all Providence College students, faculty, staff, and affiliates who interact with information technology resources. Members of the Providence College community are expected to become familiar with this Information Technology Resources Privacy Policy, to act with careful consideration of its requirements, and to seek assistance whenever necessary.

2. Purpose

The purpose of this Policy is to outline the protocols that have been enacted to ensure the privacy of non-public College data, as well as to establish the level of privacy that users can expect when leveraging Providence College information technology resources. Ultimately, this policy is intended to protect students, faculty, staff, and the College as a whole – as well as the College's vendors, partners, and affiliates – against:

- Unauthorized exposure (internally or externally) of and access to non-public College data; and
- Noncompliance with various laws and regulations.

3. Scope

This Policy applies to all students, faculty, staff and agents of Providence College, including all personnel affiliated with third parties. Additionally, this Policy applies to all IT resources owned, leased, or otherwise managed by Providence College, as well as all College data – information that is created, stored, processed and/or transmitted in the course of College operations, within or on behalf of any office or department.

4. Policy

All College Data must be used, stored, maintained, disclosed, and protected in accordance with College policies, standards, and procedures, including non-public information, PII and personal data as these terms are defined in this Policy. Reasonable efforts should be made to limit access to such records to authorized individuals only. The College may be compelled to release protected records to comply with legal obligations. Users with questions regarding maintaining privacy for non-public

information should seek guidance from their supervisor; if additional information is needed, supervisors should contact the College's Information Security Office via email: infosec@providence.edu.

4a. Maintaining Privacy Protections for PII, Personal Data, and Other Non-Public Information

- To ensure compliance with applicable laws, regulations and similar requirements, all disclosures and transmissions of non-public information must be made in accordance with **IT Security Standards** as well as applicable departmental procedures. Users should use caution when disclosing non-public information to any party via any communication medium, including the public Internet.
- New data acceptance or transmission channels, including those involving third parties, should not be established without the review and approval of Information Technology.
- Generally, when there is a legitimate business need to transmit non-public information to external entities, appropriate security mechanisms (e.g., encryption) must be utilized.
- Email and instant messaging applications do not inherently provide appropriate security measures to safeguard transmissions of sensitive and/or proprietary data. As such, non-public information should not be transmitted via these methods internally or externally.
- Non-public data should only be stored in approved electronic or physical repositories (e.g., network drives, databases, locked file cabinets, safes). The movement of non-public data from approved storage locations to unapproved storage locations (e.g., personal hard drives, flash drives, cloud storage services, etc.) requires explicit authorization.
- Approved repositories containing non-public data must be secured with controls (e.g., encryption) that are commensurate with the most sensitive type of data stored within the repository.
- Physical spaces (e.g., offices, data centers, and other computer rooms) containing non-public information stored on electronic or physical media must be appropriately secured, particularly when unattended.
- Users should only access non-public information to which they have been explicitly granted access to. Similarly, access to non-public information should only be granted to individuals who have a justified need for such access.

4b. Privacy Limitations Regarding the Use of Information Technology Resources

All users should be aware that their use of the College's IT resources is not completely private. While the College does not routinely monitor individual use of its information technology resources, the normal operation and maintenance of these resources involves:

- The backup and caching of data and communications;
- The logging of activity, the monitoring of general usage patterns, and;
- Other such activities that are necessary for the provision of service.

The College may directly monitor the activity and accounts associated with individual users of the College's information technology resources, including but not limited to, individual login sessions and communications, without notice, when:

- The user has voluntarily made them accessible to the public, by, for example, posting to an online forum, blog, or web page;

- It appears necessary to do so to protect the confidentiality, integrity, or availability of College IT resources, or to protect the College from liability or other adverse consequences;
- There is reasonable cause to believe that the user has violated, or is violating, the Acceptable Use Policy and/or policies prohibiting harassment and harmful conduct;
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
- It is otherwise required or permitted by law.

Any such active monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Vice President or the Associate Vice President for Information Technology, in consultation with the General Counsel, or their designees. The results of any such general or specific monitoring, including the contents of records of individual communications, are subject to disclosure to appropriate law enforcement agencies and/or as permitted by the Family Educational Rights and Privacy Act, as amended (FERPA). Communications made by means of College information technology resources are subject to disclosure pursuant to valid court orders and subpoenas, or other legally enforceable discovery requests. Additionally, the results of any such general or specific monitoring, including the contents of records of individual communications, can become the basis for and used in College disciplinary proceedings.

5. Procedure for Reporting an Alleged Violation of Information Technology Resources Privacy Policy

Suspected violations of this Information Technology Resources Privacy Policy should be reported in a timely fashion, in writing, to the Information Security Office. Email may be sent to infosec@providence.edu. In order to help ensure the fairness of any subsequent investigation, the individual filing the report should not discuss with or provide copies of the report to other persons. Nothing in this reporting procedure shall be interpreted to prohibit an individual from pursuing such other administrative or legal rights as he or she may have and deem necessary.

6. Enforcement

When presented with evidence of a violation of College Policy, or state or federal law, or when it is necessary to do so to protect the College against potential legal liability, the College may suspend, block, or restrict the use of its information technology resources. Violators also may be subject to other penalties and disciplinary action, up to and including probation, suspension, or dismissal.

Appendix A – Definition of Terms

- Providence College **INFORMATION TECHNOLOGY (IT) RESOURCES** as defined in the Acceptable Use Policy:
    a. **HARDWARE**: desktops, laptops, mobile devices, personally owned devices, etc.
    b. **INFORMATION SYSTEMS**: email, Banner, SAKAI, Office365, etc.
    c. **NETWORKS**: campus wired and wireless networks, other networks utilized to access College information technology resources.

d. **COLLEGE DATA**: information created, received, stored, processed and/or transmitted by the College in the course of operations; vital College assets.

- All COLLEGE DATA must be handled in accordance with College policies, standards, and procedures. Examples of sensitive College Data include:
    a. **NON-PUBLIC INFORMATION:** everything not released or otherwise made available to the general public – including but not limited to academic, financial and personnel records.
    b. PERSONALLY IDENTIFIABLE INFORMATION (PII): unique identifiers assigned or issued to a person – social security numbers (SSNs), financial account information, driver's license, passports and similar types of information not part of publicly available records.
    c. **PERSONAL DATA:** beyond PII as defined above, other types of information that can be used to identify, directly or indirectly, a person. Examples include: name, identification number, location data, and online identifiers.

Appendix B – Related Policies

- **Information Technology Acceptable Use Policy**
- **Information Technology End User Policy**
- **FERPA Guidelines**