



Information Technology

Acceptable Use Policy

Version: 1.0

Date: 03/02/2021

Policy Title: Acceptable Use 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 IT resources for the purpose of supporting its mission, goals, and values. The ability to use these resources is considered to be a privilege rather than a right. Users afforded this privilege must ensure that all such usage aligns with the standards and expectations of the College, both educationally and behaviorally.

While acceptable use of the College's IT resources is consistent with the principle of academic freedom, it also is consistent with ethical and legal expectations, as well as compliance with the policies and procedures outlined in the College Handbooks (student, faculty, staff). In other words, activities involving College IT resources that are within the sphere of academic freedom may not be considered acceptable if they do not align with Providence College's expectations, policies, and procedures.

Effective security 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 Acceptable Use 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 acceptable use of information technology resources at Providence College in order 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 non-public College data;
- Malicious activity, including the compromise of systems and services;
- Legal issues; and
- Financial loss.

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 information technology 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.



Information Technology

Acceptable Use Policy

Version: 1.0

Date: 03/02/2021

4. Policy

Key examples of permitted and prohibited activities are included in the lists below. It should be noted that these lists are not intended to be exhaustive; rather, they are meant to provide a baseline of what Providence College considers to be acceptable and unacceptable IT resource use.

4a. Do's and Don'ts - General

- **DO...** know that for security and audit purposes, authorized Providence College staff reserve the right to monitor the activity of College IT resources at any time.
- **DO...** understand that a wide variety of users, some of whom may be minors, leverage the College's IT resources.
- **DO...** use IT resources judiciously, as they are provided in support of the academic and administrative goals of Providence College. Resources are not unlimited and should be used with consideration for the rights and needs of others.
- **DO...** recognize that information distributed through Providence College's IT resources may be considered a form of publication. Users of these resources should employ appropriate language and communication methods.
- **DO...** add a disclaimer to personal statements/opinions made using a Providence College e-mail address. Unless postings from a Providence College email address to Internet forums are clearly in the course of the College's academic or administrative duties, they should contain a disclaimer stating that the opinions expressed are strictly those of the poster and not necessarily those of Providence College.
- **DO...** be mindful of personal use of IT resources, limiting use to reasonable levels using good judgment.
- **DO...** secure access to all computers, workstations, mobile devices, etc. when leaving for the day, and any other time when not actively being used.
- **DO...** take reasonable precautions to protect all passwords and other authentication data used to access Providence College IT resources.
- **DON'T...** engage in any activity that is illegal under local, state, federal, or international law.
- **DON'T...** use any resource such as email, telephone, paging, text messaging, instant messaging, or any other new electronic technologies that may emerge, to engage in any form of harassment in violation of College policy and/or applicable law.
- **DON'T...** threaten, vilify, or cyber bully others under any circumstance.
- **DON'T...** view, create, post, transmit or receive material deemed by the College obscene, unless such activity is appropriate for academic or work purposes.
- **DON'T...** use IT resources to violate the intellectual property rights held by a person or entity. This includes the downloading or use of copyright-protected music, textbooks, photographic images, motion pictures, and software for which Providence College or the end user does not have an active license.
- **DON'T...** use any resource for commercial gain, product, advertisement, or political activities unless expressly authorized by Providence College's senior management. This includes the mining of any cryptocurrency (e.g., Bitcoin) using IT resources.
- **DON'T...** make fraudulent offers of products, items, or services.



Information Technology

Acceptable Use Policy

Version: 1.0

Date: 03/02/2021

- ***DON'T...*** deliberately disrupt, corrupt, hamper, impair, infect, and/or damage the College's computer systems, networks or other IT resources.
- ***DON'T...*** knowingly execute a program that may hamper normal activities, without prior authorization.
- ***DON'T...*** access IT resources using an account belonging to another individual, or attempt to crack, brute force, capture, or guess the password of another user's account.
- ***DON'T...*** access or transmit the files or communications of other students, faculty, or staff without authorization, or provide information about, or lists of, students, faculty, staff, customers, vendors, partners or affiliates to persons, groups, or organizations outside the College without authorization.
- ***DON'T...*** use tools, software, or applications that are designed to attack, map, or determine the vulnerabilities of a Providence College computer, computer system, or network without the express consent of the Information Security Office.

4b. Do's and Don'ts - Email

- ***DO...*** be mindful of what information and attachments are sent via email. Generally, such information is not encrypted or considered to be secure during transmission over the network.
- ***DO...*** recognize that email communications using a Providence College email address are not "private" – for example, the contents may be subject to legal obligations.
- ***DO...*** use a Providence College email address when conducting official College business. Avoid the use of Providence College email when registering for personal services online.
- ***DO...*** understand that legal discovery holds may be placed on email communications, meaning that even if user deletes an email from their account, an unaltered copy of it may persist in a secure location.
- ***DO...*** immediately report suspicious emails – including those received from unknown recipients – to the IT Help Desk or the College's Information Security Office.
- ***DO...*** recognize that email storage capacity is not unlimited. Where thresholds are being approached, or exceeded, IT may contact users directly and ask them to take specific actions – for example: moving very large files to the appropriate network drive storage location prior to deletion from email account.
- ***DON'T...*** send unsolicited email messages such as "junk mail" or other advertising material to individuals who did not specifically request such material.
- ***DON'T...*** create or forward "chain letters" or other "pyramid" schemes of any type.
- ***DON'T...*** attempt to forge or spoof email accounts, messages, addresses and/or header information.
- ***DON'T...*** delete, edit, or copy files in another person's electronic messaging account (or computing device).
- ***DON'T...*** forward Providence College email to another account or address. Automated forwarding of Providence College email is not supported or allowed.



Information Technology

Acceptable Use Policy

Version: 1.0

Date: 03/02/2021

- ***DON'T...*** use a personal email account to send messages or attachments associated with official College business.
- ***DON'T...*** send credit card numbers, social security numbers, bank account/routing numbers, or other sensitive data via email (or similar instant messaging technologies).

5. Procedure for Reporting an Alleged Misuse of Information Technology Resources

Suspected violations of this Acceptable Use Policy should be reported in a timely fashion, in writing, to the College's 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 the individual may have and deem necessary.

6. Enforcement

When presented with evidence of a violation of College policies, or state or federal laws, 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 suspension, dismissal, or termination.

Appendix A – Definition of Terms

- Providence College **INFORMATION TECHNOLOGY (IT) RESOURCES:**
 - a. **HARDWARE:** desktops, laptops, mobile devices, personally owned devices, etc.
 - b. **INFORMATION SYSTEMS:** 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.

Appendix B – Related Policies

- **Information Technology Resources Privacy Policy**
- **Information Technology End User Policy**