RHODE ISLAND COLLEGE **OFFICIAL POLICY**	***Responsible Computing***	**EFFECTIVE DATE/REVISION HISTORY:** *Original policy adopted 1997/05/09; revised policy effective 2025/03/24*
RESPONSIBLE OFFICE: *Information Technology Services*	**POLICY OWNER:** *Assistant Vice President for Information Technology Services*	**LINK TO HOME PAGE OF RESPONSIBLE OFFICE**

PART 1. RATIONALE

In support of its mission of teaching, research, and public service, Rhode Island College provides members of the college community with computing and related information technology resources. The purpose of this document is to update and streamline the college's original Policy for Responsible Computing that was drafted on December 15, 1995 and approved by Council May 9, 1997.

PART 2. INTRODUCTION

This policy sets forth guidelines for the acceptable use of computing resources at the organization. It aims to ensure that these resources are used effectively, responsibly, and in compliance with all applicable laws and organizational standards.

PART 3. SCOPE

This policy applies to all members of the Rhode Island College community who use the college's computing and information technology resources, including students, faculty, staff, and authorized guests.

PART 4. DEFINITIONS

Computing Resources	All technology resources including computers, mobile devices, networks, software, and data storage systems provided by the organization.
Users	Employees, contractors, and any other individuals granted access to the organization's computing resources.
System Administrator	For the purposes of this policy, the System Administrator is the Assistant Vice President for Information Technology Services and all persons working under his or her specific direction.

PART 5. STATEMENT OF POLICY

Policy for Responsible Computing at Rhode Island College

A. All members of the college community who use the college's computing and information technology resources must respect the rights of others, including the right to confidentiality; uphold the integrity of the resources, facilities, and system controls; and comply with all pertinent laws, including contractual obligations.

B. Access to the college's computing resources is a privilege granted to RIC students, faculty, staff, and authorized guests. The college reserves the right to limit, restrict, or extend computing privileges and access to its computing and information technology resources.

C. College computing resources shall be used for the college-related activities for which they are assigned. Absent extraordinary circumstances, these resources may not be used for non-college related commercial purposes, other related activities, or personal use, other than incidental and infrequent personal use that:

1. does not interfere with the employee's job or other responsibilities.

2. does not interfere with others' use of campus computing resources.

3. complies with all other college policies and guidelines.

D. Accessing information without proper authorization, other unauthorized use of college computing resources, or intentionally corrupting or misusing information resources is prohibited. Such acts may also be crimes or civil offenses.

1. Access to sensitive or restricted information is granted on a strict need-to-know basis.

2. Users are prohibited from sharing their authentication credentials. Multi-factor authentication is required for accessing critical systems.

3. Any attempts to circumvent security measures or unauthorized access may be subject to disciplinary action.

PART 6. PROCEDURES

A. All persons using the college's computing resources, including hardware, software, networks, computer accounts, and any other information technology resources, shall:

1. use only those computing resources and computer accounts for which they have authorization.
2. use resource-shared computer accounts only for the purpose(s) for which they have been issued.
3. use college-owned computers and related equipment for college-related projects only, other than limited personal use.
4. be responsible for all use of their accounts and for protecting the password of each account.
5. immediately report any incidents involving the loss, theft, or compromise of organizational data or computing resources
6. cooperate with system administrator requests for information about computing activities.
7. take reasonable and appropriate steps to honor all hardware and software license agreements.
8. ensure that all non-college produced electronic publications that promote college programs make no implication that the publication is an official college product. When possible, the use of a disclaimer is strongly advised.

B. All persons using the college's computing resources, including hardware, software, networks, computer accounts, and any other information technology resources, *shall not*:

1. circumvent or attempt to circumvent normal resource limits, logon procedures, and security regulations.
2. transmit fraudulent information or access other users' hardware, accounts, or files without the users' explicit permission.
3. violate any software license agreement and or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
4. use the college's computing resources in a way that violates laws pertaining to harassment and/or threatening behavior.
5. physically interfere with other users' access to the college's computing resources.
6. disclose or remove proprietary information, software, printed output, or magnetic media.
7. encroach on others' use of the college's computing resources by excessive or disproportionate use of said resources.
8. disclose or remove electronic data without the explicit permission of the owner.
9. read other users' information, files, or programs without the owner's explicit permission.
10. use the college's computer facilities to violate any policy of the college, or to violate any municipal, state, or federal law.

11. use the college's technology resources for non-college related commercial purposes or for personal financial or other gain, nor shall such resources be used to solicit for or promote non-college related non-profit or political entities, groups, or organizations.

12. store, process, transmit, or access Restricted or Internal information through non-IT-approved methods or capabilities. Approved methods may include secured cloud storage services, encrypted email solutions, and authorized data transfer protocols. For detailed guidance on proper information handling practices, users should refer to the Information Handling Guide.

PART 7. Roles and Responsibilities

A. Users

1. Users must comply with all requirements and procedures defined in this policy, ensuring their actions align with the organization's standards for responsible computing.

2. Users must secure their authentication information and promptly report any suspected breach of security or misuse of resources to the Help Desk.

3. Users are responsible for adhering to all licensing agreements and respecting copyright and intellectual property laws when using organization-provided computing resources.

B. System Administrator

1. If a System Administrator observes an abuse of computing resources, or an unusual degradation of services, or receives a complaint of computing abuse or degradation of services, he or she shall take steps to maintain the integrity and performance of the system(s).

2. When engaged in the appropriate and necessary maintenance of the college computing resources, or when investigating a suspected abuse of computing, a System Administrator shall normally ask a user's permission before inspecting that user's hardware, software, or files. However, users of the college's computing resources may expect no absolute right of privacy in their use of these systems, and all college computing resources may be inspected without prior notice to users in those cases where the user is not readily available to be notified or where notifying the user would, in the judgment of the System Administrator, impede an investigation of computer abuse.

PART 8. RESPONSIBILITIES

Responsible Official	List of Responsibilities
System Administrator	Policy enforcement

PART 9. CONTACTS

Subject	Office or Position	Telephone Number	Email
Policy Clarification	AVP Information Technology Services	(401) 456-8200	avpis@ric.edu

PART 10. POLICY ENFORCEMENT

Violation(s)	Identified in Part 6 and in Part 7, Sections A and B of this policy.
Potential consequences	The System Administrator may suspend or restrict a user's computing privileges during the investigation of a problem, and upon determining that the user has violated this policy may recommend to the user's superior, or in the case of a student, to the appropriate dean, that the user's privileges be suspended or restricted for a specific period of time or permanently. A user may appeal such a suspension or restriction through normal administrative and academic channels. Depending on the severity of the infraction, other consequences identified in state and federal law include the potential for civil litigation or criminal prosecution.
Where to report violations	System Administrator

PART 11. FORMS/TEMPLATES/REFERENCE DOCUMENTS

Digital Millennium Copyright Act of 1998, *et seq*. (Federal copyright law)
R.I.G.L. § 11-52 Computer Crime
R.I.G.L. § 11-52.1 Internet Misrepresentation of Business Affiliation Act
R.I.G.L. § 11-52.2 Software Fraud
R.I.G.L. § 11-52.3 Online Property Offenses