| | |
|---|---|
| Policy Owner: | Vice President for Information Services and Technology and Chief Information Officer |
| Last Revised: | 03 / 2017 |
| Last Full Review: | 03 / 2017 |
| Contact: | Division of the Chief Information Officer, 518-276-2122 |

# Cyber Citizenship Policy

## Contents

# 1 Introduction

Cyber citizenship refers to what it means to be a participant in the online or cyber community, or to be a user of information networks and their resources. The privilege to access and use Rensselaer's information resources, systems, and networks includes certain responsibilities and obligations. It is subject to Institute policy and to local, state, and federal laws and regulations. It is also subject to a set of core Institute values that honor principals of ethics, academic integrity, academic freedom, and other community standards.

## 1.1 Purpose and Scope

This policy describes the rights, privileges, responsibilities, and obligations of the Rensselaer community with respect to the use of Rensselaer's network and its information resources and services (whether owned by Rensselaer or provided via Rensselaer's relationship with a third party) and with respect to participation in the cyber community of the Internet. It is the overarching Rensselaer policy for cyber citizenship. Unit-level policies, procedures, guidelines, and agreements must be consistent with the tenets of this policy; units may supplement, but not relax nor contradict, the restrictions, responsibilities, and obligations established herein.

The policy applies to all faculty and staff members and to all students of the Institute, individually or as groups where appropriate. It also applies to all others to whom access to Rensselaer network or information resources and services is granted.

# 2 Policy

Rensselaer's network and its information resources and services (hereafter referred to as Rensselaer information systems) are provided to serve the education and research missions of the Institute and to facilitate performing its business functions. Individuals and groups are granted access to Rensselaer information systems to further those purposes.

The remainder of this policy describes, in general terms, who may be authorized to use Rensselaer information systems and what latitude those authorized may have, again in general terms, as to what are and what are not permitted activities. *Conditions of Use* and similar policy statements may further restrict what may be allowed for specific Rensselaer information systems.

Information technology and how it is used are ever-evolving, so no policy such as this can anticipate every possible contingency, nuance, or future development. This policy, instead, will rely on general principles of ethical behavior and good citizenship in its application to unanticipated situations. The Chief Information Officer has the authority to adjudicate disputes in the interpretation of this policy.

# 3 Appropriate Use and Authorized Users

Appropriate use should always be ethical, reflect academic integrity and other community standards, show restraint in the consumption of shared resources, and be in compliance with Rensselaer's policies and government laws and regulation. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy and to freedom from intimidation, discrimination, harassment, and unwarranted annoyance. Appropriate use of Rensselaer information systems includes instruction, independent study, authorized research, independent research, communication, and official work of the offices, units, recognized student and campus organizations and agencies of the Institute.

Appropriate use may be further defined by *Conditions of Use* or similar statements for specific elements of Rensselaer information systems. Who may be authorized to use Rensselaer information systems depends on the characteristics and purpose of the resource or service. Some by their very nature are intended for use by anyone without specific authorization (such as the Rensselaer web site). Others (e.g. Rensselaer's email service) are provided to all the members of the Rensselaer community (faculty, staff, and students) while still others are restricted to a specific subset of the community (for example, a departmental file server).

The Chief Information Officer is vested with the overall authority to authorize the use of Rensselaer information systems and for the conditions of that use. Those who are authorized must be (1) current faculty members, staff, and students of the Institute; or (2) others whose use is consistent with the mission of the Institute and whose usage does not interfere with access to resources by others.

For resources and services managed at the unit level, the Chief Information Officer may delegate responsibility to the managing unit, both for defining appropriate use and designating authorized users. In all cases, though, both the authorization and the conditions of use must be consistent with the education, research, and service mission of the Institute, and be consistent with this policy.

# 4 Responsibilities and Privileges

Each member of the campus community is accountable for his or her actions as a condition of continued membership in the community. The interplay of privileges and responsibilities engenders the trust and intellectual freedom that form the heart of our community. To maintain this trust and freedom, each person must develop the skills necessary to be an active and contributing member of the community.

Authorized users must fulfill certain obligations as part of and in their use of Rensselaer information systems. Similarly, there are fundamental privileges common in the academic community, several with counterparts in the cyber world. These responsibilities and privileges are found in the following list, but it must be understood that no privilege is absolute nor without limitation. Additional detail and clarity where appropriate appears in subsections after the list.

a) Authorized users of Rensselaer information systems must be mindful of the impact their use may have on others with legitimate interest in using Rensselaer information systems.
b) Authorized users of Rensselaer information systems must protect the authentication credentials they use when accessing Rensselaer information systems.
c) Authorized users of Rensselaer information systems must be responsible stewards of the resources to which they have access.

d) Authorized users of Rensselaer information systems are responsible for the proper maintenance, security, and compatibility of their devices connected to the Rensselaer network or used to access Rensselaer information systems.
e) Authorized users of Rensselaer information systems must report any cyber security event through the appropriate Rensselaer channels and cooperate in any investigations.
f) Principles of academic freedom extend to the use of Rensselaer information systems by authorized users.
g) Principles of expectation of privacy extend to the use of Rensselaer information systems by authorized users.
h) Principles of ownership for intellectual work products extend to the use of Rensselaer information systems by authorized users.
i) Individuals must abide by reasonable administrative directives issued by Rensselaer from time to time concerning the access or use of Rensselaer information systems.

## 4.1 Responsible Use of Resources

The use of the Rensselaer information systems must be consistent with the mission and values of the Institute and in compliance with the normal standards of civil, ethical and legal behavior. Rensselaer information systems are assets shared by the Rensselaer community. As such, individuals should be mindful of the impact their own activities may have on others and their use of information resources. Individuals must be respectful of the finite capacity of the resources, and refrain from consuming excessive amounts of network bandwidth or other system utilities. Incidental personal use, including recreational, is permitted provided it does not impede the legitimate activities of others and is not otherwise prohibited by the unit in control of the resource.

## 4.2 Protection of Access Credentials

The use of Rensselaer information systems granted to an authorized user is for that person's sole use. Generally, access credentials (e.g. user identifier and password) are needed to identify the authorized user and enable access to the resource. Authorized users are responsible for the security of their access credentials. Access credentials must not be shared with others.

## 4.3 Information Stewardship

Authorized users of Rensselaer information systems may, as part of their authorized use, have access to information resources belonging to Rensselaer or others. Use of the information must be limited to what is authorized, and in addition the authorized user must not handle the information in a way that puts it at risk of alteration or deletion or exposure to others not authorized to access the information.

Moreover, even when confidential information is exposed inadvertently, individuals should respect the confidentiality the information warrants.

## 4.4 Devices

Devices connected to the Rensselaer network or used to access Rensselaer information systems should be compatible with the purpose and capabilities of the Rensselaer information systems and should have their software components well-maintained. Devices with unsupported operating systems or application software, or lacking applicable security patches, are vulnerable to cyberattack. They put themselves at risk of data breach or worse; they also put the rest of Rensselaer's network at risk of data breach or worse.

Individuals are responsible for devices they use to access Rensselaer information systems and for devices they connect to Rensselaer's network. Devices that are not compatible with capabilities of the Rensselaer information systems or its purpose or that are improperly maintained or which show signs of compromise from a cyberattack may be isolated from the rest of the Rensselaer network or removed from the network entirely and denied access to Rensselaer information systems.

## 4.5 Security Incident Response

Cyber space is an astoundingly rich resource of information, products, and services. It is also astoundingly hostile to unsuspecting people and equipment. Attacks attempting to exploit vulnerable computer systems or to lure individuals into scams or frauds are continual. No amount of due-diligence can protect everything that needs to be protected all the time. Every now and then, an attempt will succeed.

Individuals are obligated to report all suspected security incidents. An investigation may be required to assess the impact of the suspected incident; individuals are required to assist with any such investigation.

The Chief Information Officer through his or her Information Security Office is responsible for promulgating procedures for responding to security incidents.

## 4.6 Freedom of Expression

In keeping with its long tradition of academic freedom, Rensselaer supports free inquiry and expression in the use of Rensselaer information systems. Rensselaer, however, reserves the right to take action against or deny access to its facilities to those whose use is not consonant with the purposes of the university or infringes on the rights of others.

## 4.7 Privacy

Rensselaer acknowledges that privacy is an important value for educational institutions. Creative, innovative, and risky thought—as well as scholarship and educational accomplishment—all depend on interacting in a communication context in which individuals feel free to express and transmit their opinions and ideas.

Thus, Rensselaer extends to its authorized users a reasonable expectation of privacy in their activities using Rensselaer information systems. However, everyone should recognize that privacy cannot be guaranteed, even when it is intended. While Rensselaer does not monitor the online activities of individual authorized users, individual privacy may be compromised in an unintentional, incidental way during routine information system operation or maintenance, and it may be infringed in a more deliberate way when so authorized with cause.

Rensselaer may access or disclose activity log records for an individual or group using Rensselaer information systems or the information files or communications stored on or transmitted by Rensselaer information systems (1) when there is reason to believe Rensselaer policy has been violated, (2) to preserve Rensselaer rights and assets, or (3) when compelled by legal process. The determination is made by the appropriate vice president with the concurrence of the Chief Information Officer.

### 4.8 Ownership of Intellectual Works

Individuals creating intellectual works using Rensselaer information systems, including but not limited to software, should consult *The Rensselaer Intellectual Property Policy* available online at https://research.rpi.edu/sites/default/files/TheRensselaerIntellectualPropertyPolicy_0.pdf.

## 5 Prohibitions

Prohibited activities involving Rensselaer information systems are found in the following list. Additional detail and clarity where appropriate appears in subsections after the list.

a) Individuals must not share passwords or other access information or devices or otherwise authorize any third party to access or use Rensselaer information systems on their behalf.
b) Individuals must not engage in unlawful or illegal activity nor activity in violation of Rensselaer policy.
c) Individuals must not engage in any unauthorized access or unauthorized use of Rensselaer information systems.
d) Individuals must not use Rensselaer information systems to breach or violate any confidentiality obligations or privacy requirements, including by collecting or harvesting confidential information.
e) Individuals must not use Rensselaer information systems to misappropriate or violate the rights of any third party, including using Rensselaer information systems to store, receive, send, or make available materials protected by intellectual property rights of third parties without the permission of the owner of the intellectual property rights, unless otherwise permitted by applicable law.
f) Individuals must not damage, disrupt, tamper or interfere with, diminish, or render inaccessible or unusable Rensselaer information systems, Rensselaer's or others' equipment, software, data, communications or use of Rensselaer information systems, or attempt to do so, or encourage or assist others to do so.
g) Individuals must not initiate a denial of service attack from or against Rensselaer information systems or release a virus, Trojan horse, worm or other malware or spyware from or against Rensselaer information systems.
h) Individuals must not use Rensselaer information systems to engage in fraudulent activity nor to perpetrate a hoax or engage in phishing schemes or forgery or other similar falsification or manipulation of data.
i) Individuals must not use Rensselaer information systems to abuse, harass, stalk, threaten, cyber bully, unlawfully discriminate against, or otherwise violate the rights of others nor to libel or defame others.
j) Individuals must not resell or charge others for Rensselaer information systems, either directly or indirectly, except as authorized by Rensselaer.
k) Individuals must not take any action that encourages or assists others in engaging in any acts prohibited under this policy (including providing others with the ability to access data or resources they should not be able to access).
l) Individuals must not use Rensselaer information systems to misrepresent their identity or impersonate any person.

m) Individuals must not use Rensselaer information systems to participate in pyramid schemes or chain letters.
n) Individuals must not use Rensselaer information systems for commercial purposes that are unrelated to Rensselaer in an official way.

## 5.1 Conduct and Misbehavior

The tenets of cyber citizenship are founded in the tenets of ordinary citizenship. Standards of behavior for the Rensselaer community apply both to real-world actions and to those committed in a cyber context.

No individual may use Rensselaer information systems to violate Rensselaer policy or the law. Cyber bullying is still bullying. Online snooping is still invasion of privacy. Neither the unique abilities nor the sense of anonymity possible online empower individuals to misbehave.

## 5.2 Unauthorized Access

All use of Rensselaer information systems must be authorized. Except for those cases where the information systems are intended for general public use (e.g. Rensselaer's web presence), the authorization must be explicit.

No individual may use Rensselaer information systems without authorization, nor may Rensselaer information systems be used to access the information systems of others in unauthorized ways. This prohibition is not limited to just the information system itself; it extends to the information stored on, processed by, or transmitted to or from the information system as well.

The absence of an effective access control may not be interpreted as authorization to access a system or resource. Individuals must not attempt to circumvent an access control, and they must not examine, alter, copy, nor delete information resources without a reasonable expectation that permission to access the resource was intended.

### 5.2.1 Privileged Access

Staff personnel with responsibilities for the maintenance, operation, and administration of Rensselaer information systems may be granted special privileges needed to perform their job responsibilities. Individuals with special privileges may use them only to the extent necessary to reasonably perform the duties of their position.

No one may exploit a special privilege or ability to monitor the activities of any individual or group in their use of Rensselaer information resources, to intercept information in transit, nor to examine, alter, copy, or delete information resources belonging to other authorized users except where explicitly authorized according to this policy.

## 5.3 Intellectual Property

Intellectual property is fundamental asset for any university. Rensselaer requires its property rights in research results, inventions, course design, and all other results of scholarly pursuit be respected. To complement this requirement, Rensselaer requires that the intellectual property rights of others be respected as well.

Intellectual property rights most commonly fall under copyright, patent, trademark, or non-disclosure agreement, but regardless of the protection, Rensselaer information systems must not be used to infringe on the intellectual property rights of others.

### 5.3.1 Copyright

Copyright applies to certain forms of creative works such as literary and artistic production. Included under copyright protection are books, maps, reports, and other publications, and also such things as sound recordings, films, photographs, software, and architectural works. Copyright includes the right to reproduce, distribute, publish (which is interpreted broadly to include perform or display), and to create derivative works of the original. The rights granted to the copyright holder are exclusive, but they are not absolute. The rights are exclusive in the sense that others are prohibited from using the work without the holder's permission, but they are not absolute because there are limitations and exceptions, most notably under the principle of *Fair Use*.

Use of material protected by copyright requires either the permission of the copyright holder or an exemption under *Fair Use*. Guidance regarding copyright and for applying the principles of *Fair Use* may be found on the Rensselaer Libraries website at http://library.rpi.edu/update.do?catcenterkey=71.

### 5.3.2 Software

Software falls under copyright, but distribution is typically not by the sale of copies of the work. Instead, the software is licensed for use under a set of terms and conditions. Software products must not be installed or used on Rensselaer information systems unless they are properly licensed for the purpose.

Special caution is required for products that are available in "personal use" or "trial" versions. Personal-use editions are often restricted to non-commercial use by an individual on personally-owned equipment at home. Software of this sort must not be used on Rensselaer information systems.

Trial versions may forbid any sort of production use. The trial version is intended for evaluating the software product for some purpose, not for conducting the business of the organization. Trial-version software must not be used on Rensselaer information systems for other than the permitted purpose.

### 5.3.3 Entertainment

The intellectual property of the entertainment industry (e.g. music, television, motion picture) falls under copyright. However, the ease with which digital copies of material can be made and then distributed without regard to the copyright holder's intention has made intellectual property "piracy" an especially acute problem for the entertainment industry.

The entertainment industry has been aggressive in defending its rights. On occasion, this has led to lawsuits seeking substantial sums of money in damages for copyright infringement. Individuals should be aware that the legal consequences for piracy rest on the individual, not the university.

## 5.4 Personal Use

Personal use of Rensselaer information systems falls outside of their broad purpose. Personal use is generally not allowed except (1) where the activity is incidental in nature both in terms of resource consumption and the financial value of the activity, (2) does not impede the legitimate activities of others using Rensselaer information systems, (3) does not interfere with employee work responsibilities, and (4) is consistent with community standards and all other Rensselaer policies.

Personal use for the benefit of any commercial third party is prohibited, as is facilitating access for a third party to Rensselaer information systems for which the third party would not otherwise have authorized access.

Special exemptions may be granted for activities deemed aligned with Rensselaer's interests. The Chief Information Officer has the authority to grant exemptions.

### 5.5 Misrepresentation

No one may use electronic communication, including its various forms as social media, in an attempt to impersonate another person or otherwise misrepresent oneself to others. Although there are instances in which anonymous communication (or communication under a fictitious identity with no intent to deceive) is acceptable, it is generally advisable to identify oneself accurately.

## 6 Relationship to Other Policies

The *Cyber Citizenship Policy* is an Institute-wide policy. It supersedes all previous policies on the same subject. This policy has a peer relationship with other Institute-wide policies where it is primary for the specifics of activities involving Rensselaer's network and its information resources and services; others are primary for their respective areas.

a) Faculty, Employee, and Student Handbooks – These policy documents define elements of acceptable and unacceptable behaviors by the faculty, staff, and student body, respectively. Those elements must be consonant with this *Cyber Citizenship Policy*. The handbooks also specify how violations of policy, including this policy, are adjudicated.
b) Intellectual Property Policy – This policy defines the terms and conditions for ownership and protection of intellectual property created by members of the Rensselaer community.
c) Conditions of Use statements – Components of the Rensselaer information system may have explicit statements delineating how the individual systems may be used, usually in line with the intended purpose of the systems. The statements may be more restrictive than the *Cyber Citizenship Policy*, but they still must be consistent with it.

## 7 Reporting Violations

Questions that may arise about this policy or whether something would violate its tenets may be directed to the VCC Help Desk.

Except as provided otherwise in this policy, suspected incidents that would violate other Institute-wide policy should be reported in accordance with the other policy. Some violations of this *Cyber Citizenship Policy* will have no clear parallel in other policy (or the parallel may be unknown), in which case suspected violations may be reported to Public Safety.

## 8 Enforcement and Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including, but not limited to, the loss of access to Rensselaer's network and its information resources and services, disciplinary action, dismissal from the Institute, and legal sanctions.

Incidents involving students, faculty members, or staff members will be handled according to procedures found in the respective handbooks for students, faculty, and staff and guidelines established

by the Vice President for Student Life, the Provost, or the Vice President for Human Resources, as appropriate.

Some violations may constitute criminal offenses. These may be referred to local, state, or federal authorities for prosecution.

# 9 Approval

This policy is approved under the authority of the President of Rensselaer Polytechnic Institute.

| {original signed} | June 27, 2017 |
|---|---|
| Signature | Date |

Dr. Shirley Ann Jackson