ACCEPTABLE USE POLICY

ACCEPTABLE USE POLICY

Purpose

This policy outlines the acceptable use of information resources at Roxbury Community College and applies to employees, contractors, consultants, temporaries, and other staff at Roxbury Community College, including all personnel and affiliated via third party contractors. This policy applies to all data and equipment that is owned or leased by Roxbury Community College. The purpose of this policy is to protect employees, partners and the College against internal and/or external exposure of confidential information, malicious activity, including the compromise of systems and services, legal issues, financial loss, and damage to reputation by individuals, either knowingly or unknowingly.

Scope

Personnel using data and information resources (including but not limited to Internet/Intranet/Extranet-related and core systems, computer equipment, software, operating systems, storage media, and network accounts providing electronic messaging), must use them for business purposes in accordance with their job functions and responsibilities, serving the interests of the College and the customers in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

Policy

It is the responsibility of every user of information resources to know the Information Security Policies and the acceptable use of information resources, and to conduct their activities accordingly.

General Use

- Safeguard user accounts and passwords, and use them only as authorized
- Respect all pertinent licenses, copyrights, contracts, as well as other restricted and proprietary resources
- To accommodate employees, Roxbury Community College understands employees will access the Internet for personal needs periodically
- It is expected that employees will exercise good judgment regarding the reasonableness of personal use and any question regarding appropriate use will be decided by management
- Notify the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents
- Secure all unattended workstations from unauthorized viewing or use
- All workstations must be configured to automatically lock after 15 minutes of inactivity and users should log off or lock their machines during extended periods of inactivity.

Unacceptable Use

- Damaging computer systems
- Preventing another user from authorized resources
- Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties
- Revealing account passwords to others. Employees who receive usernames and passwords must keep their usernames and passwords confidential and must not share that information with others.
- Using another person's computer account, with or without their permission
- Providing information about employees to parties outside
- Employees are forbidden to install software on their computers without the prior approval of their supervisor
- Procurement of or use of any Software as a Service (SaaS) providers without the approval of Information Technology (see POL-23 System-Acquisition & Development Policy)
- Implementation of any information technology component, product or service without the approval of and involvement from IT
- Removing software from systems, unless assigned as a job requirement or prior consent from Information Technology is obtained
- Providing protected customer or vendor information to any unauthorized person
- Intentionally corrupting, misusing, or stealing software or any other computing resource
- Sending unsolicited (spam) electronic messaging (e.g., email) and chain letters
- Forging electronic messaging header information
- Using electronic messaging, telephone or other communication method, to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile workplace laws
- Accessing, editing, deleting, copying, or forwarding files or communications of another user in any media (e.g., paper, electronic, video, etc.), unless assigned as a job requirement or with prior consent from the file owner
- Deleting, editing, or copying files in another person's computer or electronic messaging account
- Illegal use, including duplication or distribution of copyrighted or College proprietary material, including electronic, hardcopy, audio, and video in any medium
- Employees are forbidden to install software on their computers without the prior approval of their supervisor
- Procurement of or use of any Software as a Service (SaaS) providers without the approval of Information Technology (see POL-23 System-Acquisition & Development Policy)
- Implementation of any information technology component, product or service without the approval of and involvement from IT
- Removing software from systems, unless assigned as a job requirement or prior consent from Information Technology is obtained
- Circumventing any of the information security measures of any host, network or account without officer approval for emergency business purposes
- Using resources for personal benefit
- Introducing malicious programs into the information systems
- Unauthorized modification of configuration files
- Knowingly executing a program that may hamper normal activities, without prior authorization
- Operating a wireless network or allowing other computers to connect to your computer wirelessly
- Employees must not reveal any information about the College's clients or employees which is not already publicly available without expressed permission from their manager
- Unauthorized disclosure of confidential information to individuals outside the College and to individuals within the College without a business need, legal or regulatory requirement
- Disclosure of Personally Identifiable Information (PII) such as social security numbers, bank/credit card numbers, driver's license/id numbers, etc. and any other information classified as confidential, personal or sensitive to any unauthorized individual within the College without a business need
- Disclosure of PII to any individual outside of the College unless there is a legal or regulatory requirement
- Unencrypted transmission of PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information and financial account numbers such as in the body of or an attachment to an electronic message, via FTP, via instant messenger or via fax
- Storing confidential information including PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information or financial account numbers on laptop computers and mobile computing devices unless no alternative exists and then it must be encrypted
- Downloads from the internet are strictly forbidden. If downloads are required for business use, contact IT and arrangements may be made
- Under no circumstance is an employee authorized to engage in any activity deemed illegal by international, federal, state, or other local laws while utilizing College assets

- Under no circumstances may an employee disable anti-virus software or alter anti-virus software settings
- Under no circumstances may an employee disable firewall software or alter firewall software settings
- Employees should not open any electronic messaging attachments that are not expected, or are from unknown addresses, or appear in any way suspicious
- Employees must not use College accounts to post publicly accessible messages or posts.
- Employees may not perform vulnerability scans, monitor network traffic, attempt to elevate rights or privileges, or gain access to information not expressly intended for them
- Employees must be extremely cautious about the use of instant message applications, as these applications are insecure. Sensitive information must not be shared through this mechanism.
- To ensure compliance with this policy, Roxbury Community College may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any Roxbury Community College's information resources consent to disclose the contents of any files or information stored or passed through Roxbury Community College's equipment. All data contained on or passing through the College's assets is subject to monitoring and remains the property of the College at all times.

Other provisions

- Explicit management approval must be provided for use of IT resources by employees or third parties
- Explicit management approval is required to add a new device to the network
- Authentication is required to use any technology
- Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties
- A list of all devices and personnel with access shall be maintained
- Devices will be labeled with owner, contact information and purpose
- A list of acceptable uses of technology and acceptable network locations shall be maintained
- A list of College approved products shall be maintained

Enforcement

- Personnel using Roxbury Community College's information resources in opposition to this policy may be subject to limitations on the use of these resources, suspension of privileges (including internet access), as well as disciplinary and/or legal action, including termination of employment.
- Employees, contractors, consultants, temporaries, and all personnel affiliated via third parties shall sign an agreement to comply and be governed by this policy and the Roxbury Community College Information Security Policies upon hire and again annually.
- For employees with access to credit card data or sensitive information, background checks will be performed.

Related Regulations

This policy is a component of Roxbury Community College information security program that is intended to comply with the PCI-DSS, FERPA, Gramm Leach Bliley Act and other regulations.

Exceptions

Only the Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy.

Violations

Any user found to have violated this policy may be subject to disciplinary action, up to and including notifying the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

A Supervisor, Department Manager, Dean, or Vice President will address violations of this policy by staff members and have full authority to sanction an immediate stop to the actions in question. Appeals from any formal disciplinary action taken against a unit professional staff member will be governed by their specific contractual grievance procedure. The Complaint Procedure of the Board of Higher Education Non-Unit Professionals Personnel Policies will govern non-unit staff. The Vice President of Enrollment Management and Student Affairs will address violations of this policy by students.

Disclaimer

The College makes no warranties of any kind, whether expressed or implied, with respect to the information technology services it provides. The College will not be responsible for damages resulting from the use of communication facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a College employee, or by the user's error or omissions. Use of any information obtained via the Internet is at the user's risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official College record. The College also does not accept responsibility for removing material that some users may consider defamatory or otherwise offensive. Users should be advised, however, that dissemination of such material may subject them to liability in other forums.