

ACCEPTABLE USE POLICY

ACCEPTABLE USE POLICY

QA 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.

- QA
- QA 2
- QA 3

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