Rowan College
of South Jersey

Administrative Procedure: 4001
ACCEPTABLE USE OF TECHNOLOGICAL RESOURCES
(Collaboration Platforms, Email Enterprise Information System, Internet, Social Media, and Off-Campus Portable Presentation Equipment)

Overview

Appropriate and inappropriate use of the College's technological resources is divided into the following five areas:

- Electronic Communications
- Enterprise Information System
- Internet Access
- Social media
- Off-Campus Portable Presentation Equipment

Electronic Communications

Email
College provided email is intended for official and authorized purposes only. Equipment and services are provided to support email use necessary to promote the College's mission, goals, objectives, and strategic plan and operations. Access to email is a privilege to which all students and employees are entitled in order to perform effectively. Responsibilities accompany this privilege and may be withdrawn; if abused.

Collaboration Platforms
Collaboration platforms enable digital workspaces where employees and students can communicate, share files, and manage projects in real-time, regardless of where they are located. The platforms enable video/web conferencing for virtual meetings, shared document editing, and instant messaging. For additional information regarding collaboration platforms, please see policy and administrative procedure 4009 Collaboration Platforms.

Use of Personal Email Accounts
Students' and employees' personal email accounts are not to be used for College academic or work-related purposes. College email accounts and personal email accounts are not interchangeable. Only the College's official email system is to be used for

academic or work-related purposes unless superseded by federal law. Password information is not to be shared.

Activation/Termination
College access is controlled through individual accounts and passwords. It is the responsibility of the employees and students to protect the confidentiality of their accounts and password information. Password information is not to be shared, and all users are responsible for all activities and data associated with their College accounts.

All employees and students are provided with an individual College account. Accounts may be granted to third-party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Board of Trustees member
- Retired employees granted emeritus status by the Board of Trustees
- Consultant
- Contractor
- Guest

Applications for these temporary accounts must be submitted to the Executive Vice President and Chief Operating Officer/Chief Financial Officer (EVP/COO/CFO) or designee via formal request using the RCSJ Ticketing System.

Account access will be terminated when employees or a third-party terminates their professional association with the College, in accordance with the Division of Innovation & Technology's standard operating procedures. The College is under no obligation to store, forward, or make available the contents of employees' or a third-party's related account information after the term of their professional association has ceased.

Student email access will be terminated in accordance with the Division of Innovation & Technology's standard operating procedures, including, but not limited to, if a student violates the terms and conditions of use, are suspended, expelled from the College, transfers, or graduates.

Appropriate Use
Students and employees must exercise good judgment in the use of electronic communications. Electronic communications are to be used for academic and work-related purposes only and not provided by the College to be used for non-work purposes.

To fulfill academic or work-related obligations, in addition to being informed of important announcements and updates, all current students and employees are expected and responsible for checking their electronic communications in a consistent and timely manner. They also have responsibility for mailbox management, including organizing and cleaning. If any users subscribe to a mailing list, it is their responsibility to be aware of how to remove themselves from the list, and to be responsible for email address changes.

Students and employees are expected to comply with professional and personal standards of courtesy and conduct.

Inappropriate Use
Since electronic communications are records of the College, users must treat messages as if they were written on College letterhead. Electronic communications (language, images, videos, or sounds) may not be used for harassment, intimidation, threatening physical harm, obscenity, pornography, libel, slander, defamation, impersonation, fraud, copyright infringement, plagiarism, computer tampering (e.g., spreading computer malware), nor any other illegal or unlawful purpose.

Employees may not use College electronic communications to disseminate information on any non-College activities including, but not limited to, political events, religious observances, charitable events/fund-raising (unless College approved), and other personal business.

It is the responsibility of the user to contact Technical Support if an inappropriate or suspected phishing message is received from an internal or external source.

Distribution
Distribution of messages to all users or sub-set(s) of all users will be through the College's intranet.

Messages intended for all users will be considered a Campus Announcement. All Campus Announcements must be submitted for approval three (3) business days prior to the intended posting to the College's intranet.

Messages intended for groups of users will be considered Group Announcements. Group Announcements can be posted by College employees identified as group leaders, when they have been given administrative authorization to post messages for a specific user group.

Text Messaging
The College must comply with the Telephone Consumer Protection Act (TCPA). Therefore, the College can only send text messages to individuals that have given their express consent to receive text message communication through a College approved messaging service. For the safety of the College community, and in accordance with federal law, emergency communications cannot be opted out of.

Non-College Use
Use of the College's email and collaboration platforms is expressly for activities related to teaching and learning and conducting those activities necessary to perform one's assigned duties and professional development activities as College employees or students. At times, a private for-profit or a private not-for-profit entity without College affiliation may wish to use the College email to distribute information, request information, conduct fund-raising, or communicate with College personnel. Requests for

these services must be directed to the EVP/COO/CFO or designee, whose determination on these matters will be final.

No Expectation of Privacy/Ownership
Users must be aware they have no expectation of privacy when using any College provided email or collaboration systems. All emails and messages sent through College systems are the property of the College. The College reserves the right to access and disclose all messages sent or received using its messaging systems to determine whether users have breached security, violated College policy, or engaged in other unauthorized or illegal actions.

Electronic communications and other data sent over College-provided systems are College records. As College records, digital content may be requested and released without notice to either the sender or receiver under certain state and federal laws. Electronic correspondence may also be subpoenaed and used as evidence in court cases.

Additionally, while the College Information Technology staff does not actively read end-user email or other electronic correspondence, messages may be inadvertently viewed during the normal course of system management.

Employees and students using College systems must note that "deleting" an electronic message or digital content does not necessarily erase it from the computer network. Backup copies of electronic messages may exist, despite end-user deletion, in compliance with the College's technology resource management procedures. The goals of these backup and archiving procedures are to ensure system reliability and prevent data loss.

Safeguards are implemented and routinely assessed to ensure that any review of electronic messages has a legitimate and authorized purpose.

Acceptable Communication
Official administrative or academic business is the only type of acceptable communication via email or collaboration platforms. This includes communications directly related to the College's mission, goals, objectives, and strategic plan. The sender must be mindful of two main concerns when sending such messages: (1) the number of recipients is to be appropriately limited to minimize the waste of recipients' time that results from distributions that are overly broad; and (2) each electronic mail message creates a record that is composed to contribute effectively to the College's work. College email is not for employees' or students' personal use.

Responses to Electronic Mail
When responding to an electronic mail message, employees and students must avoid replying to "all recipients," unless appropriate. Responses should not be made to all recipients routinely.

In general, when the original message is addressed to a tailored group, such as a team working on a matter, and the response would be of interest to the whole team, the "all

recipients" response is appropriate. However, when all recipients of a message have no reason expect a response, the response should be directed only to the sender.

The College reserves the right to automatically delete all email located in the delete or junk folders on a regular basis.

Failure to Comply
Any user who misuses the College's electronic communication platforms will be subject to disciplinary action. Sanctions for inappropriate use may include, but not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all technological resources or services;
2. Disciplinary action according to applicable College policies; and/or
3. Legal action according to applicable laws and contractual agreements.

Disclaimer
The College assumes no liability for any direct or indirect damage arising from a user's email or other electronic messaging usage.

Additional Information
Clarification regarding the use of the College's electronic communications may be obtained from the EVP/COO/CFO or designee.

Enterprise Information System

Employees are given discrete levels of access to the College's Enterprise Information System in order to perform their job duties. It is the employees' responsibility to safeguard all data to which employees have been granted access.

Personally Identifiable Information
Personally Identifiable Information (PII) is any data that could potentially identify a specific individual including, but not limited to, social security number, date of birth, and address information. PII can be sensitive or non-sensitive data and should always be treated confidentially. If employees believe PII has been compromised, employees must immediately inform the EVP/COO/CFO or designee.

It is the responsibility of College employees who have access to PII to ensure the data is safe-guarded and used appropriately. This data is never to be sent via email, text message, or any type of instant messaging service. PII data must be stored on designated College servers or designated College platforms and NEVER stored on a local computer hard drive, laptop, or ~~a~~ portable storage device. PII should never be uploaded, imported, or shared with a third-party service or entity that does not have an established business agreement with the College. Refer to Board of Trustees Policy 8109 Student Records for additional information.

Keep Accounts Secure
It is the responsibility of employees and students to protect the confidentiality of their accounts and password information. Employees and students must never share their College username or password with anyone, or share access to their accounts, as doing so will circumvent security procedures. Employees and students are responsible for all activities associated with their College username or password. Employees and students are to ensure that Multifactor Authentication (MFA) is enabled on all supported accounts.

Internet

Appropriate and inappropriate use of the College's internet technologies is the same as described for electronic communications and applies as well to the use of the internet, the College's intranet, and emerging technologies.

Account Activation/Termination
College user accounts are treated in the same way as email accounts. See section above.

Appropriate Use
Internet access is for College business (administrative or academic) only and may not be used for personal reasons.

Employees and students are encouraged to use the Internet to further the mission, goals, objectives, and strategic plan of the College.

Activities that are encouraged include:

1. Communicating with fellow employees, business partners of the College, and within the context of individuals' assigned responsibilities;
2. Acquiring or sharing information associated with one's job or academic assignments; and
3. Participating in educational or professional development activities.

Geoblocking of Network Services
To protect the College's digital infrastructure and ensure secure access to technological resources, the College uses geo-blocking controls that restrict access to certain services based on geographic location. These safeguards are informed by cybersecurity threat intelligence and applied as needed to reduce exposure to elevated risk.

As a result:

1. Users attempting to access College systems from locations subject to geo-blocking may experience limited or restricted connectivity.
2. Users on College networks attempting to access services hosted in geo-blocked regions may also encounter limited or blocked access.

The list of locations subject to geo-blocking is maintained by the Division of Innovation & Technology and reviewed periodically in accordance with evolving risk assessments.

The current list is available in the College's Knowledge Base Article, "Geo-blocking of RCSJ Services" at:

https://rcsj.teamdynamix.com/TDClient/1944/Portal/KB/ArticleDet?ID=156971

Artificial Intelligence (AI)
Artificial Intelligence tools do not meet the College's security, privacy, and compliance standards for handling data that is not publicly available. Employees should never enter non-public institutional data or information protected by the Family Education Rights and Privacy Act (FERPA) or the Gramm-Leach-Bliley Act (GLBA) into AI tools or services that are not specifically licensed by the College. Entering data into AI tools and services that are not contracted by the College is the equivalent of posting that data on a public website. AI tools collect and store user data as part of their learning process. Any data entered into an AI tool becomes part of its training data, which it may then share with other users outside the College, and could expose proprietary or sensitive information to unauthorized parties.

Inappropriate Use
Individuals will not interfere with others' use of the Internet. Users are not to violate the network policies of any other network accessed through their College account. Users will comply with all federal and state laws, all College policies, and all contracts.

Inappropriate use includes, but not limited to, the following:

1. Using the Internet for illegal or unlawful purposes e.g., harassment, intimidation, threatening physical harm, obscenity, pornography, libel, slander, defamation, impersonation, fraud, copyright infringement, plagiarism, computer tampering (e.g., spreading computer malware).
2. Viewing, copying, altering, or destroying data, software, documentation, or data communications belonging to another individual without authorized permission.
3. Making copyrighted material available to others without permission, whether through "peer to peer" software, web sites, or other technology.

Failure to Comply
Any user who misuses College Internet access will be subject to disciplinary action. Sanctions for inappropriate use of the Internet may include, but not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all technological resources or services;
2. Disciplinary action according to applicable College policies; and/or
3. Legal action according to applicable laws and contractual agreements.

Disclaimer
The College assumes no liability for any direct or indirect damages arising from a user's College email, collaboration platforms, or connection to the Internet. The College is not responsible for the accuracy of information found in College email, collaboration

platforms, or on the Internet, and only facilitates access to and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

Additional Information
Clarification regarding the use of the College's email, collaboration platforms, and internet access may be obtained from the Vice President & Chief Information Officer.

Social Media

The College recognizes and embraces social media as a fundamental means of communication and supports its use by community members to facilitate conversation. As a public institution, the College believes it is crucial to stay abreast of trends and remain active in the social sphere to closely connect with the campus community.

Definition
The College defines "Social Media" as any online tool and service that allows a user to create and publish content on the internet. For the purpose of this administrative procedure, social media means any service for web-based and mobile publication and commentary, including, but not limited to, blogs, wikis, RSS feeds, interactive geo-location, microblogs, message boards, chat rooms, electronic newsletters, online forums, video sharing sites, social networking sites, and other websites and services that permit users to share information with others in a contemporaneous manner.

Accountability
Under the direction of the Vice President & Chief Information Officer, designated staff will ensure compliance with this administrative procedure.

Applicability
This administrative procedure applies to all faculty, employees, and students of the College who accept responsibility for engaging in work-related social media.

Purpose
This administrative procedure contains guidelines for those initiating or managing a social media presence that involves the College, its departments, programs, groups, organizations, student clubs, and individuals. It outlines how the College supports institutional communication via social media so the College's social media communications efforts remain as consistent as possible. Social media usage at the College is governed by the same policies and administrative procedures that govern all other electronic communications, technology, and the Internet and must follow the same ethical standards by which the College abides.

Guidance
- Official College social media accounts must follow the Terms of Service set forth by their respective social media channel(s). The guidelines outlined herein do not

surpass existing College policies and administrative procedures related to the use of technology, codes of conduct, or confidentiality.

- Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. These inquiries are referred to Public Relations.

- Employees and students must be aware the College may observe content and information made available through social media. Employees and students are to use their best judgment in posting material that is inappropriate or harmful to the College, its employees, students, or vendors. It is the responsibility of all end users to maintain appropriate privacy settings.

- Each end user must be aware of the effect their actions may have on their image, as well as the College's image. The information that employees and students post or publish may be public information indefinitely. Posts are to be made with care to avoid unintended legal or life-changing ramifications.

- It is required that employees and students keep College-related social media accounts separate from personal accounts, when applicable.

- End users are not to post confidential or proprietary information about the College, or College employees, students, affiliates or alumni that would violate such person's rights to privacy under applicable federal and state laws and regulations. This includes the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach_Bliley Act (GLBA), and College policies and administrative procedures. Non-disclosure agreements that prohibit the College from disclosing information prohibit its employees from disclosing such information.

- Personally identifiable information that can be used to identify an individual or affiliated/unaffiliated third party offline, including but not limited to, phone numbers, home or local addresses, social security numbers, Employee/Student IDs, birth dates and email addresses, cannot be posted. In general, a photo release form must be obtained from parties whose images are identifiable to post, share, or distribute. This does not include photos from the College's archives or those obtained by College representatives, whose original intent was for distribution.

- Rights and permissions must be secured before posting, sharing or distributing copyrighted materials, including but not limited to, music, art, photographs, texts, portions of video, or information considered proprietary by a College partner, vendor, affiliate, or contractor.

- Personal communication via social media is not exempt from the laws and regulations that govern personal liability across general and traditional forms of

communication. Such communication does not indicate that an individual is speaking on behalf of the College and is to clearly identify the individual's personal communications. Employees who use personal social media channels to talk about work or College-related manners are asked to disclose their affiliation with the College and may consider adding a disclaimer to personal social media accounts stating their thoughts are their own.

- Employees may occasionally utilize social media and the web for personal matters in the workplace. Employees may engage in incidental personal use of social media in the workplace so long as this use does not consume significant time or resources, interfere with operations and productivity, or violate College or department policies.

- Violations of this administrative procedure may require the suspension or removal of any social media account(s) at the purchaser's expense and possible disciplinary action. A disciplinary or other review may be initiated if employees' online activities violate law or College policy or administrative procedure, or if individuals' non-official or unauthorized online activities otherwise subject the College to liability for such acts.

- The College reserves the right to monitor use of its computer systems.

Additional Guidelines for All Technology Use

Improper Use of Copyright and Proprietary Information of Others
Failure to observe software copyrights and/or license agreements may result in disciplinary action by the College and/or legal action by the copyright owner. Any copyrighted content submitted or used with the consent of the copyright owner is to contain a phrase such as "Copyright owned by [Name of Owner]; used by permission."

Commercial Purposes
College information and computing resources are not to be used for commercial purposes.

Use for Unauthorized Purposes
Users are not to utilize the College's email, electronic communications, collaborative platforms, internet access, or social media for personal or private business, product advertisement, political lobbying, or to distribute or promote religiously oriented information.

Use of Rowan College of South Jersey Name
The College's name may not be used, without the College's prior written consent, the name "Rowan College of South Jersey" or any symbol, logo, or graphic used by or associated with the College or any confusingly similar symbol, logo, or graphic as part of an email address, a home page, or a domain name for any online network utilized,

originated, or registered with the Internet or similar authority. To obtain consent, contact Public Relations.

Online Conduct
Online networks are to be used only as permitted by the College, in accordance with applicable College policies, and for lawful purposes. Users are prohibited from posting on or transmitting through any email, internet, or social media site anything that is illegal or unlawful including harassment, intimidation, threatening physical harm, obscenity, pornography, libel, slander, defamation, impersonation, fraud, copyright infringement, plagiarism, computer tampering (e.g., spreading malware), which encourages conduct that would constitute a criminal offense, gives rise to civil liability, or otherwise violates any applicable law or College policies.

More specifically, the following conduct violates College policies and is not permitted and subject to disciplinary action. Such conduct includes, but not limited to:

- *Harassment* - Targeting another individual, group, or organization to cause distress, embarrassment, injury, unwanted attention, or other substantial discomfort is harassment and prohibited. Personal attacks, actions to threaten, intimidate or embarrass an individual, group or organization or attacks based on a person's race, ethnicity, handicap, religion, gender, veteran status, sexual orientation or another such characteristic, or affiliation are prohibited.

- *Impersonation* - Communication under a false name or designation the user is not authorized to use, including instances in conjunction with representing that an individual is somehow acting on behalf of or under the auspices of the College is prohibited.

- *Chain letters and pyramid schemes* - Transmission of chain letters and pyramid schemes of any kind are prohibited. Certain chain letters and pyramid schemes are illegal.

- *Excessive use of bandwidth* is prohibited. Examples include, but not limited to, game playing, participating in peer-to-peer file sharing, and downloading large multimedia files.

- *Disruption of network users, services, or equipment* - Disruptions include, but not limited to, distribution of unsolicited advertising, propagation of computer malware, unauthorized access to any other computer or system and any unauthorized action with the effect of denying access to a system or service.

Reporting Violations

While the College will do everything possible to provide quality technological resources, it is the employees' and students' responsibility to ensure that their technology experience here at the College is a productive one.

If at any time, employees or students feel their rights as ~~a~~ technology users are being violated or if they are aware of other users who are misusing or abusing the technological resources, they are urged to promptly report the problem to the appropriate College official, such as the Vice President and Chief Compliance Officer or Vice President & Chief Information Officer. With timely knowledge of the incident, the issue can quickly be investigated and resolved.

The College must comply with the Patriot Act (Public Law 107-56) and any other current and future federal and state law that regulates electronic mail and technology use. This may mean that data compiled through the use of the College network may be released to federal and/or state authorities under appropriate legal protocols.

Off-Campus Portable Presentation Equipment

Employees may request the use of portable presentation equipment (such as projectors, speakers, and microphones) for use in College-related functions that take place off-campus.

- Requests for equipment must be approved by the Division of Innovation & Technology's Instructional Technology office at the relevant campus. A minimum of three (3) business days is required for all requests. All requests must include a pickup date and return date.

- All equipment loans must be evaluated in accordance with the priority of regular College needs.

- Any damage to loaned equipment is the financial responsibility of the division or group to which the borrower reports.

- It is the responsibility of employees to promptly return equipment at the conclusion of the loan.

Area: Innovation and Technology
Approved: 07/01/19
Revised: 04/21/26

President's Authorization: 

References:

Rowan College of South Jersey Board of Trustees Policy Manual, *4001 Acceptable Use of Technological Resources (Email, Enterprise Information System, Internet, Social Media, & Off-Campus Portable Presentation Equipment); 4009 Collaboration Platforms; 7011 Harassment and Discrimination; 8003 Anti-Bullying and Intimidation*, and *8109 Student Records*

Rowan College of South Jersey Administrative Procedure, *4009 Collaboration Platforms; 7011 Harassment and Discrimination; 8003 Anti-Bullying and Intimidation* and *8109 Student Records*