



## Rowan College of South Jersey

Administrative Procedure: 4001

### **ACCEPTABLE USE OF TECHNOLOGICAL RESOURCES**

(Email, Enterprise Information System, Internet, Social Media, and Off-Campus Portable Presentation Equipment)

#### **Overview**

Appropriate and inappropriate use of the College's technological resources are 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 Responsibilities accompany this privilege and may be withdrawn, if abused.

##### Use of Personal Email Accounts

Student and employee 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 Only the College's official email system is to be used for academic or work-related purposes unless superseded by federal law.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 email 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 work accounts.

All employees and students are provided with a College email account. Email accounts will 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;
- Professor Emeritus;
- Retiree;
- Consultant;
- Contractor; or
- Guest.

Applications for these temporary accounts must be submitted to the Vice President and Chief Information Officer (VP/CIO) or his/her designee. All terms, conditions, and restrictions governing email use must be in a signed agreement which the VP/CIO will provide.

Email access will be terminated when the employee or third party terminates his/her professional association with the College, unless other arrangements are made. The College is under no obligation to store or forward contents of an employee's or third-party's email system after the term of his/her professional association has ceased.

Student email access will be terminated when the student violates the terms and conditions of use, or is suspended or expelled from the College. Student email may be terminated when the student graduates.

#### Appropriate Use

Student and employee email users must exercise good judgment in the use of email. Email is to be used for academic and work-related purposes only and is not provided by the College to be used as a personal email account.

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 email 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.

College student and employee email users are expected to comply with professional and personal standards of courtesy and conduct.

#### Inappropriate Use

Since email messages are records of the College, email users must treat email messages as if they were written on College letterhead. Email (language, images, 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 email 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 email 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 intranets. The Gloucester campus primarily utilizes the Ellucian Portal as its intranet while the Cumberland campus primarily utilizes Blackboard as its intranet. Campus Announcements and Group Announcements are also available via the campus intranet for distribution of messages to all users and user groups.

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

Messages intended for groups of users will be considered Group Announcements. Group Announcements can be posted by the College employee identified as a group leader, when he/she has 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.

#### Non-College Use

Use of the College's email 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 a College employee or student. 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 VP/CIO or his/her 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 messaging 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 mail and other messages sent over College provided systems are a College record. As College records, email and other messages 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 and other electronic correspondence, messages may be inadvertently read by staff during the normal course of managing systems.

Employees and students using the College electronic mail system must note that "deleting" an electronic message does not necessarily erase the message from the computer network. Backup copies of electronic messages such as email and text 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 business (administrative or academic) is the only type of acceptable communication via email or messaging systems. This includes communications directly related to the mission, goals, objectives, and strategic plan of the College. 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 take care not to respond to "all recipients" of the previous message unless it is appropriate to do so. Responses are to never 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 to receive responses, the response is to only be directed 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 electronic mail or messaging systems 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 resource 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 email or other electronic messaging usage.

*Additional Information*

Clarification regarding the use of the College's electronic mail may be obtained from the VP/CIO or his/her 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 responsibility of each employee to safeguard all data to which the employee has been granted access.

*Personally Identifiable Information*

Personally Identifiable Information (PII) is any data that could potentially identify a specific individual such as, 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 in a confidential manner. If an employee believes PII has been compromised the employee must immediately inform the VP/CIO or his/her designee.

It is the responsibility of the College employee whom has access to PII to assure 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.

*Keep your Username and Password secure*

It is the responsibility of employees and students to protect the confidentiality of their accounts and password information. Employees are to never share their College username or password with anyone as doing so will circumvent security procedures. Employees are responsible for all activities associated with their College username or password.

## Internet

Appropriate and inappropriate use of the College's internet technologies are the same as described for electronic communications and apply as well to the use of the World Wide Web, the College's campus intranet, FTP (File Transfer Protocol), 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.

Employee 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 an individual's assigned responsibilities;
2. Acquiring or sharing information associated with one's job or academic assignments; and
3. Participating in educational or professional development activities.

### 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 resource 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 connection to the Internet. The College is not responsible for the accuracy of information found on the Internet and only facilitates accessing 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 internet access may be obtained from the Vice President & Chief Information Officer.

### **Social Media**

The College recognizes and embraces that social media is a fundamental shift in the way people communicate and supports the use of social media by its community members as a way to facilitate communication and 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 allow an Internet user to create and publish content. For the purpose of this administrative procedure, social media means any facility for web-based and mobile publication and commentary, including, but not limited to, blogs, wikis, RSS feeds, interactive geo-location, microblogs such as Twitter, message boards, chat rooms, electronic newsletters, online forums, video sharing sites such as YouTube and Vimeo, social networking sites such as Facebook, LinkedIn, Instagram, Snapchat and other sites 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) 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 locate an individual or affiliated/unaffiliated third party offline, including but not limited to, phone numbers, home or local addresses, social security numbers, Banner IDs, birth dates and email addresses, are not 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 matters 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 an employee's online activity violates law or College policy or administrative procedure, or if an individual's non-official or unauthorized online activity otherwise subjects 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, 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 and downloading large multimedia files such as MKVs.
- *Disruption of network users, services, or equipment* - Disruptions include, but not limited to, distribution of unsolicited advertising, propagation of computer malware, and using the network to make unauthorized entry to any other computer or computer system accessible via the network.

## Reporting Violations

While the College will do everything possible to provide quality technological resources, it is the employee's and student's responsibility to ensure that his/her technology experience here at the College is a productive one.

If at any time, an employee or student feels that his/her rights as a technology user are being violated or if he/she is aware of other users who are misusing or abusing the technological resources, he/she is urged to promptly report the problem to the appropriate College official, such as the Special Assistant to the President Diversity and Equity/Title IX Compliance 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

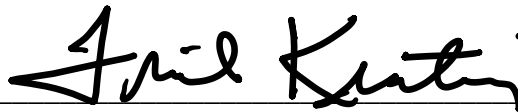
Employees may request the use of portable presentation equipment (such as projectors, speakers, and microphones) for use in College-related functions that take place off-campus.

- Requests for equipment must be approved by the Division of Innovation & Technology's Instructional Technology office at the Gloucester campus. A minimum of one business day 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.

Area: Innovation and Technology

Approved: 07/14/20

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)*; *7011 Harassment and Discrimination*; and *8003 Anti-Bullying and Intimidation*.

Administrative Procedure: 4001 Acceptable Use of Technological Resources