**Rocky Mountain College's Computer Use Policy**

1. **Introduction**

Rocky Mountain College's (RMC) Information Technology (IT) resources consist of assets such as computer equipment, software, networks, computer system accounts and other digital assets and resources that primarily support the academic and administrative functions of the College. These assets are either owned by RMC or used by RMC under contract with an external provider. The use of these assets are governed by federal and state laws as well as RMC policies, regulations and rules.

1. **General Use of IT Resources and Regulatory Limitations**
	1. RMC computer accounts are for the exclusive use of the individual to whom they were assigned, and users may not allow or facilitate unauthorized access to RMC computer accounts or IT resources by others. For example, users may not allow unauthorized access to restricted resources by sharing their password or other methods.
		1. Students and employees of the RMC receive computer accounts and are authorized users of IT resources unless access privileges have been revoked.
		2. Departments may request guest and temporary accounts for authorized use of IT resources by non-College personnel. The department that is responsible for the guest and temporary accounts must ensure that this regulation is understood and adhered to by the users of the accounts.
	2. Use of IT resources must comply with federal and state laws, and RMC policies, regulations and rules.
	3. Use of IT Resources provided to RMC under a contract with an external provider are also subject to the terms and conditions of the contract with the provider.
	4. RMC may examine the content of both personal and work-related electronic information stored or archived on IT resources. The examination will be requested in writing by the President, a Vice President or their delegates and then approved by the Director of HR. An examination of these records may be undertaken for any of the following purposes:
		1. To ensure the security and operating performance of its IT resources.
		2. To ensure compliance with College policies, regulations or rules, or state or federal law.
		3. To perform audit-related activities.
		4. To comply with E-discovery rules relating to an actual, threatened or potential lawsuit, with a subpoena, or with other court orders.
		5. To address an imminent threat to health or safety.
		6. To conduct authorized College investigations.
	5. Computer users should have no expectation of privacy with regard to any personal material stored or archived on IT resources. The IT staff will respect personal privacy where practical, users who want to ensure that their personal materials are not subject to College access are advised to use their own personal, non-College equipment, networks and storage.
		1. RMC may monitor and examine personal IT resources which contain College records/data for the reasons specified above in Section 2.4. This includes, but is not limited to, the application of Section 6.3 of this Regulation.
	6. RMC may authorize confidential passwords or other secure access identification.
	7. The IT staff may use active measures to detect compromised machines and identify vulnerable services so long as the active methods are low risk and concerns are reported to appropriate users.
	8. For information related to College business, a supervisor or other designated official may have appropriate access for work-related purposes. No permission or approval from the user is needed for such access (see section 2.4). If personal and business information are not clearly separated, the designated official may examine all information to the extent needed to separate and access business information for work-related purposes. President or Vice Presidents may approve rules to exclude personal files from storage on network drives, in which case all files and data on the affected systems may be treated as information related to College business.
	9. Authorized IT personnel reserve the right to examine server/desktop “log” information to identify computer users and the electronic addresses to which they have connected (e.g., Web sites or e-mail) to the extent consistent with privacy laws and necessary for College business purposes.
	10. RMC reserves the right to limit or revoke access to IT resources when policies, regulations or rules, or state or federal law are violated or where contractual obligations or operations may be impeded. Attempts will be made to notify the affected user(s).
	11. All material prepared and utilized for purposes of RMC business and posted to or sent over IT resources must be accurate and must correctly identify the sender, unless an administrator (department head or higher) approves anonymity for a College business purpose.
	12. Any traffic on the IT resources may be monitored by authorized personnel for research purposes. Access to information content will be consistent with policies, regulations or rules, or state or federal law, and the purpose for which the traffic is being monitored.
	13. Employees using IT resources cannot convey personal statements that could be construed as representing the positions or beliefs of the Institution. For example, religious views, political campaign positions, proselytizing remarks and quotations are not allowed in e-mail signature blocks.
	14. Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup or archival purposes, may be a violation of copyright law.
	15. Users of IT resources, including computer systems, must take appropriate security precautions to protect and secure data residing in or on assigned College accounts or other IT resources. These precautions include ensuring that security patches are applied to software products, and adhering to any security guidelines, standards or regulations for any device (RMC-owned or personal) that accesses RMC data and services. A violation of any security guideline, standard or regulation shall be considered a violation of this regulation as outlined in Section 5.
2. **Personal Use of IT Resources**
	1. Authorized users may access IT resources for occasional, inconsequential personal uses, with no expectation of privacy, if the following conditions are met:
		1. The use does not negatively impact the availability or performance of the IT resources.
		2. The use does not otherwise negatively inhibit, impact or detract from the users’ work performance or the work performance of other employees.
		3. The use does not seek or result in an employee’s commercial gain or private profit, except as allowed under applicable intellectual property or external activities for pay regulations.
		4. The use does not violate any licensing agreements or any law or policy on copyright and trademark.
		5. The use does not state or imply sponsorship or endorsement unless allowed by another applicable policy.
		6. The use does not otherwise violate policies, regulations or rules, or state or federal law.
		7. The use does not involve unauthorized passwords or the abuse of identifying data and/or tools that attempt to circumvent system security or that in any way attempt to gain unauthorized access.
		8. The use does not involve sending or soliciting chain letters, nor does it involve sending unsolicited bulk mail messages (e.g., "junk mail," or "spam," or "MLM.").
		9. The use does not result in any direct cost to the College.
		10. Any creation of a personal World Wide Web (WWW) page or a personal collection of electronic material that is available to others must include a disclaimer that reads as follows: "The material located at this site is not endorsed, sponsored or provided by or on behalf of Rocky Mountain College."
3. **Use of IT Resources for Commercial, Advertising and Broadcast Purposes**
	1. No paid advertising will be allowed on official College web sites. However, an RMC web site may contain a simple acknowledgment of sponsorship by an outside entity in the following form: "Support for this web site has been provided by \_\_\_\_\_\_\_\_\_\_\_\_\_." The acknowledgment may include the sponsorship's logo only if permission is granted by the sponsor, and the use of the logo does not imply commercial endorsement by the College.
		1. An "official College web site" is any World Wide Web (WWW) address that is sponsored, endorsed or created on authority of a College department or administrative unit. Web sites on College servers are either "College web sites" or personal web sites allowed by the College.
		2. "Paid advertising" means advertising or promotional information provided in exchange for legal consideration, including money or other valuable benefits.
	2. Personal web pages that are hosted on RMC-owned computers will not contain paid advertising.
	3. While College employees may post messages to newsgroups, blogs, chatrooms or other Internet resources dedicated to advertising, the messages may not refer readers to a College telephone number or College e-mail address.
	4. Computer account holders can not send mass e-mail messages without prior approval from the President, Vice President's, Director of Information Technology or their designees. The use of e-mails by offices to reach their users will not be considered mass e-mail under this section. The use of authorized College e-mail lists for their intended purpose will not be considered mass e-mail under this section.
	5. Registered trademarks of the College may be used in the Web sites of computer account holders on the conditions that (a) they are not used for or related to private profit or commercial purposes, and (b) they do not mislead or confuse viewers as to whether the Web page is College-sponsored.
	6. The President or designee may approve specific exceptions to the prohibition on paid advertising.
4. **Violation of Policies, Regulations or Rules**
	1. Any violation of applicable policies, regulations or rules regarding use of IT Resources by employees will be "misconduct" under RMC policies (faculty and non-faculty), or "unacceptable personal conduct" under RMC policies. For students, violations are "misconduct" under the applicable student disciplinary code. For approved guests, violations will result in appropriate action depending on their affiliation. Violators are subject to appropriate disciplinary procedure, and violations of law will also be referred for criminal or civil prosecution. Sanctions may include removal of access privileges in addition to other sanctions available under RMC's regular disciplinary policies.
	2. Apart from disciplinary procedures, an authorized IT system administrator may suspend a user's access privileges or suspend services to a computer for as long as necessary to protect the IT resources, to prevent an ongoing threat of harm to persons or property, or to prevent a threat of interference with normal College functions. As soon as practicable following the suspension of access, the system administrator must take the following actions:
		1. The user must be sent written or electronic notice of the suspension of access and the reasons for it, along with whom the suspension may be discussed.
		2. The user must be given an opportunity to meet with the system administrator or his/her designee in a timely manner to discuss the suspension and present any reasons the user has why the suspension should be lifted. The system administrator must reconsider his or her suspension decision in light of the information received at this meeting.
		3. Following the meeting, the user must be sent a written or electronic copy of the system administrator's decision upon reconsideration, and must be notified that he/she may appeal to the system administrator's immediate supervisor if the user is dissatisfied with the outcome of the meeting.
5. **Application of Records Rules**
	1. Duty to preserve records: All information created or received for College work purposes and contained on IT resources, RMC's electronic mail (e-mail) systems, or on privately owned devices are property of RMC. As with hard-copy documents, the retention of e-mail messages will be in accordance with applicable public records law and RMC's published guidelines regarding records retention and disposition. The College will utilize a centralized email archive that retains email indefinitely.
	2. Additional duty regarding records requests and potential litigation: Any RMC employee or authorized guest (e.g., volunteers and students serving as a work study) who receives a record request, possible lawsuit or other legal claim must promptly (a) notify the Director of HR of the request or possible claim and (b) locate and preserve all relevant records.
	3. Duty to provide access to information content: Employees and approved guests with a network account or RMC computing device must provide appropriate assistance for access to information content (including decryption and entry of passwords). This assistance should only be provided when an identified official (e.g., supervisor, person in employee's supervisory hierarchy) needs access to any of RMC's records/data the employee may have stored on RMC machines, systems or storage devices, or on non-College machines, systems or storage devices. Any failure to provide an identified RMC official access to information content on RMC machines, systems or storage devices, or non-College machines, systems or storage devices that may contain the RMC’s records/data shall be considered a violation of this regulation as outlined in Section 5.
		1. Access to e-mail archives: The only persons who can access archived email is the employee and the Director of Information Technology. The Director of Human Resources will be the only person that can request access to the e-mail archive. Access to the archived emails must be from a Court ordered e-discovery or in connection with an HR action outlined in 6.3.2. In this case, none of the employee's personal (non-work-related) email would be copied. Student e-mails will never be accessed unless a Court ordered e-discovery is received.
		2. Procedures to access e-mail archives: All requests for access to e-mail archives must be in writing and approved by the Director of Human Resources. The Director of Human Resources along with the Director of Information Technology will be the only persons accessing the archive. These requests will be maintained by the Director of Human Resources and will be verified through the uses of a quarterly access audit produced by the e-mail archive system.
6. **Additional Rules**
	1. Additional rules on computer use may be adopted by various divisions/departments to meet specific administrative or academic needs. Any adopted requirement must:
		1. Comply with applicable federal and state laws;
		2. Be consistent with the policies and regulations of Rocky Mountain College;
		3. Be adopted and posted in writing or electronically in a manner that is available to all affected users.
		4. Be filed with Director of Human Resources and the Director of Information Technology.