ACCEPTABLE USE OF TECHNOLOGY POLICY

I. Policy Section

6.0 Human Resources

II. Policy Subsection

6.18 Acceptable Use of Technology

III. Policy Statement

GRCC grants access to one or more forms of technology to employees, students, and other individuals or entities affected by this policy. GRCC owns this technology and any use and communication from this technology, including internet access granted by GRCC, should not be considered confidential. This policy is not intended to abridge academic freedom or the constitutional guarantees of freedom of speech or freedom of expression. The use of technology, including connections to networks outside of GRCC and social media will be in accordance with the guidelines presented within this policy.

IV. Reason for Policy

This policy is enacted to ensure the use of technology and social media adheres to applicable government regulations and laws, as well as the College's mission and business practices, including but not limited to, policies, procedures, and standards relating to ethics, confidentiality, and professional conduct.

V. Entities affected by this Policy

Employees
Students
Trustees
Guests
Volunteers
Vendors
General Public

VI. Who should read this Policy

Employees
Students
Trustees

Guests
Volunteers
Vendors
General Public

VII. Related documents

GRCC Technology Acceptable Use Agreement
GRCC Personally Identifiable Information Policy
GRCC Copyright Policy
Conflict of Interest Policy
Student Code of Conduct

VIII. Contacts

Policy Owner: Chief Information Officer
General Counsel
Director of Communications
Executive Director of Human Resources
GRCC Chief of Police

IX. Definitions

1. College Network - Grand Rapids Community College internal network: any device that receives an internal, routable IP address from a wired, wireless, or VPN connection is considered to be on the Grand Rapids Community College internal network. Special designated and segmented networks may be available for unmanaged devices.

2. Technology - includes, but is not limited to, the following: Personal computers, file servers, hardware, software, e-mail, telephone systems, cell phones, cameras, voicemail, fax machines, printers, Internet and Web-based systems, wireless networks, and any other resources provided by the College to students, staff and faculty.

3. Unmanaged device - any device (laptop, workstation, mobile device, IP camera, alarm system, etc.) that GRCC Information Technology does not manage.

4. Conduct - includes all ways in which students and employees manage themselves in any context, including in person or through the use of technology.

5. Social Media and Social Networking - includes online communities where users can create a profile for themselves, and then socialize

with others using a range of tools including but not limited to posting to blogs, tweeting, video, images, tagging, lists of friends, posting to forums and messaging.

6. For the purpose of this policy, “users” are the staff, faculty, students, guests, volunteers, and vendors who use the technology resources of Grand Rapids Community College. For the purposes of this policy “Social Media” and “Social Networking” do not include online business networking activities that comply with GRCC’s acceptable use agreement.

X. Procedures

1. Technology resources are procured and provided solely for business purposes. GRCC discourages personal use of technology provided by GRCC during office hours but acknowledges certain circumstances when this cannot be avoided. Users shall not use computer or telecommunication systems in such a manner as to degrade or disrupt the normal operation of voice/data networks and college computer systems. Users shall not intentionally damage or disable computing, telecommunication equipment or software or circumvent user authentication or security.

    a. Acceptable Use Agreement: Responsibilities for users in the use of the College’s technology resources are outlined in the Technology Acceptable Use Agreement (AUA). All users must agree to the AUA before accessing GRCC technology resources.

    b. Users shall comply with all applicable user conduct codes and rules, laws and regulation governing the use of computer and telecommunication resources. Examples include the GRCC AUA agreement, laws of libel, privacy, copyright, trademark, obscenity, child pornography, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.

    c. Unmanaged devices shall not connect to the College Network due to the risk of impacting the confidentiality, integrity, and availability of the College Network, devices, and data. The Information Technology Division shall develop procedures that aid to enforce this policy. Exceptions may be permitted through a review process. GRCC Information Technology reserves the right to revoke any permitted exceptions at any time.

    d. At any time and without prior notice, GRCC reserves the right to monitor, inspect, or search all GRCC owned information systems. This examination may take place with or without the consent,

presence, or knowledge of the involved individual(s). The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voice mail files, printer files, fax machine output, and other College property such as desk drawers and storage areas. All communication and data may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Communication and data using GRCC technology is subject to potential disclosure under the Freedom of Information Act.

e. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by management, employees are prohibited from engaging in, or attempting to engage in breaching the confidentiality of another person's communications such as using another person's login and password.

f. Posts by users to social networking sites are governed by GRCC's policies, including the Conflict of Interest Policy and the Student Code of Conduct. Employee and Student behavioral standards shall apply to all conduct, whether in person or online.

g. While performing services for GRCC, unless otherwise specified in an employment contract, individuals must grant to GRCC exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop. All programs and documentation generated by, or provided by individuals for the benefit of GRCC are the property of GRCC. GRCC asserts the legal ownership of the contents of all information systems under its control. GRCC reserves the right to access and use this information at its discretion.

2. Procedure for Investigating Policy Violations:

a. Violations of this policy should be reported to an employee's immediate supervisor as well as one or more of the following:

i. Chief Information Officer
ii. Chief Information Security Officer
iii. Executive Director of Human Resources
iv. GRCC Chief of Police
v. General Counsel

b. Alleged violations will be investigated. Additional agencies may be notified and involved in the investigation and resolution depending on the individual circumstances. These agencies may include GRCC Police, local law enforcement and other State and Federal authorities.

3. Enforcement of Policy:

Any violation of this policy may result in disciplinary action, up to and including, discharge from employment. Additionally, violators of this policy may also be subject to civil or criminal sanctions as provided for by law.

XI. Forms

GRCC Technology Acceptable Use Agreement

XII. Effective Date

February 1, 2011

XIII. Policy History

December, 2010: policy revisions included policy name change to ensure the policy encompasses all forms of technology and social media policy provisions.

March, 2017: no changes

April, 2023: Added definitions regarding “College Network” and “Unmanaged Devices”

XIV. Next Review/Revision Date

April, 2027