Technology Acceptable Use Agreement

This Technology Acceptable Use Agreement pertains to the use of Grand Rapids Community College (GRCC) information technology, telecommunications resources, and other digital technologies. The College provides these resources specifically to support its mission and its business processes. The Acceptable Use Agreement Policy provides definitions and procedural details referenced in this agreement.

The College Network provides access for its students, employees, volunteers, vendors and clients (hereafter referred to as the user) to local, state, national, and international information technology resources through connections with networks outside GRCC. It is the responsibility of those external networks to enforce their own acceptable use agreements and policies. GRCC accepts no responsibility for network traffic that violates the acceptable use agreement of any directly or indirectly connected networks beyond informing the user of a potential violation if the external network so informs GRCC.

All users accessing the College Network, as well as the Internet, are responsible for adhering to codes of conduct, rules, laws and regulations governing the use of computer and telecommunication resources. Examples include but are not limited to laws of libel, privacy, copyright, trademark, obscenity, child pornography, the Electronic Communication Privacy Act and the Computer Fraud and Abuse Act. Any attempt to violate existing laws through the use of the College Network may result in criminal charges and/or litigation against the offender by the proper authorities. If such an event should occur, GRCC will comply fully with authorities to provide any information necessary for the litigation process.

Campus computer systems and the College Network resources are the sole property of GRCC. All messages, documents, and other forms of information created, sent, or received by any user under this agreement using GRCC information technology resources may be accessed, reviewed, and disclosed by GRCC at any time without prior notice or consent from the user or the party from whom a transmission is received. Under no circumstances should a user expect or understand that any digital information, e-mail message, or any attachment thereto, sent by GRCC e-mail systems or Internet service or information accessed by GRCC systems is confidential. The user has no expectation of privacy under this agreement. Disclosure may include, but is not limited to, officials of law enforcement, regulatory bodies, and governments as well as members of the general public making requests under the Freedom of Information Act. Further, such messages, documents, and information may be subject to compulsory disclosure through the judicial process. Once computer accounts are closed, access to the accounts or the data contained within them may be granted to others to facilitate transfer of responsibility or the retrieval of data. GRCC does not warrant the functionality or performance of the resources made available by the use of computer and network accounts to meet particular purposes or usages, and the user who holds such accounts bears the entire risk of loss or damages arising there from.

Employees are responsible for the reasonable care and security of the computer system components that they are assigned or use. Employees will promptly report any equipment, software and data damage, destruction or theft. Employees may be subject to discipline and held financially responsible for any equipment or data that is lost, stolen or damaged because of the employee's negligence, misuse or abuse (Examples of negligence include: leaving equipment in unlocked vehicles or repeatedly spilling liquids on computer equipment).

Use Agreement

From the time a user receives a network and/or computer systems account, the user is solely responsible for all actions taken while using that account. In particular, it is a violation of this agreement to:

- Apply for an account under false pretense
- Assume another person's identity without proper authorization
- Communicate under the identity of any entity without proper authorization from that entity
- Grant access to the account, with or without sharing credentials, to any other person. If an account is shared with another person, the account holder will be held responsible for the actions of the other person
- Delete, exam, copy, or modify files and/or data belonging to other users or the College, without their prior written consent
- Attempt to evade or change the resources allocated to a computer or network account
- Continued impedance of other users through mass consumption of system resources after receipt of a request to cease such activity
- Use computing and network facilities and/or services for commercial purposes
- Engage in an unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction
- Intentionally access known pornographic or obscene information or to engage in use of remote computer sites where gambling for money is practiced
- Illegally share copyrighted materials. More information regarding copyright law can be found at: www.copyright.gov
- Connect an Unmanaged Device to the College Network; exceptions may be permitted through a review process by the IT Division. GRCC Information Technology reserves the right to revoke any permitted exceptions at any time.

Electronic Mail

- Forge (or attempting to forge) electronic mail messages
- Read, deleting, copying, or modifying the e-mail of another or the attempt to do so
- Send harassing, obscene, offensive, disruptive, and/or other threatening e-mail to another person or the attempt to do so
- Send or forwarding unsolicited junk mail, a commercial or "for-profit" message, or a chain letter or the attempt to do so

- The user must comply with all state and federal privacy laws and GRCC's policies regarding privacy, confidentiality, and proprietary information

Network Security

- Use the College Network to gain unauthorized access to remote systems
- Use the College Network to connect to other systems by or through the evasion of the physical limitations of the local or remote system
- Decipher (i.e., decrypt) system or user passwords
- Copy any system files
- Disregard applicable copyright laws
- Attempt to secure a higher level of access privilege on the College Network than was granted
- Probe or scan the College Network
- Willfully introduce a computer "virus" or other type of "malware" program that may be disruptive or destructive into any GRCC computer system or network or into any external network

Social Networking

- Engage in social networking using GRCC technology for any commercial or significant personal use
- Post information which is confidential and proprietary to the College
- Post material that is threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity
- Promote or advertise a commercial product or solicit business or membership or financial or other support in any business, group or organization for personal gain

Acceptance and Acknowledgment

I understand that any violation of this agreement will result in disciplinary action which may include but is not limited to the following: written discipline, revocation of the user's accounts, termination of employment, suspension, or expulsion from GRCC and/or legal action taken by GRCC. Permanent revocations may result from recommendations by the Information Technology division of GRCC or other authorities which may be called upon to investigate computer and/or network abuse. Disciplinary action, as documented in GRCC Policies and Procedures, any applicable collective bargaining agreement or handbook and/or the GRCC Student Code of Conduct, will be determined solely by GRCC according to the nature of the violation.