Adirondack Community College

Acceptable Use of Information Technology Resources

# Objective

To ensure Adirondack Community College (ACC) and all of its users are protected from illegal and/or harmful actions that result from inappropriate use of College systems, and to ensure that all users are responsible for proper use of identified Systems.

# Definitions

Data: All information used by the College in its academic or business operations.

Confidential Data: Information that includes, but is not limited to, student or employee records (social security number, ID number, grades, financial data, account numbers, bills, employee performance reviews, personnel files, personal information), business data (credit card numbers, account information, passwords, etc.), and any other information deemed confidential by ACC.

Protected Data: Confidential data that is encrypted, password protected or stored on encrypted drives.

Systems: This applies to all technology equipment and data owned or supported by ACC which includes, but is not limited to, computers and mobile devices and any data contained on them, external storage devices, printers, network and server resources such as Banner, Angel, internet access, e-mail, file shares, software, system/user accounts.

Users: All College faculty, staff and students, in addition to all authorized guests that access or use technology resources.

# Responsibilities of Users

# The College makes every attempt to ensure that data, systems, and users are protected from any illegal and/or harmful activity. However users should be aware that the College cannot guarantee security and confidentiality. Therefore it is the responsibility of all users to ensure proper use of College systems including:

1. Use that is efficient and consistent with the College mission, values, policies, manuals, handbooks, and standard/best practice guides.
2. Use which consistently protects the confidentiality, integrity, and availability of data. This includes the responsibility of all users to:
	1. Ensure that data is accurate, including the prevention of any defacement or mishandling;
	2. Ensure that access to data is restricted based on the needs of a job function, and ensure that proper authorization has been granted for all data that is accessed;
	3. Ensure that data is available for appropriate users;
	4. Ensure that confidential data is rigorously protected and used solely for College use.
3. Use that complies with federal, state and local law (including, but not limited to, all laws outlined in the Legal Standards section below), including copyright and intellectual property rights as well as license agreements and contracts.
4. Immediately contacting the Chief Information Officer (CIO) if you believe your account may have been compromised or have witnessed any violations of this policy.

# Privacy & Monitoring

The College reserves the right at any time to monitor and access any data, including the contents of any College computer or College communication, for any legitimate business or legal reason. Portions of the technology infrastructure include automatic and manual monitoring and recording systems that are used for reasons that include, but are not limited to, security, performance, backup, and troubleshooting.

1. **Personal Use**

The College reserves the right to restrict personal use of College systems. While these systems are provided for College use only, the College recognizes that occasional, brief personal uses of computers may be necessary from time to time to attend to personal matters that cannot be handled outside work/school hours. Personal use of systems must not interfere with or disrupt any College business or educational use. Use of personal equipment on the wireless network is allowed.

# Prohibited Behavior

1. Circumvention of any security systems and/or procedures, including any unauthorized activities aimed at compromising system or network security, including: hacking, probing, or scanning; attempts to break into other users' accounts or to obtain passwords; use of computer viruses, worms, or any kind of spyware or malicious software.
2. Sharing your username or password with another person, or using another’s account name or password; using your College password with any non-college system.
3. Storing non-protected confidential data on non-college systems.
4. Removing/transmitting/copying non-protected confidential data from College systems without authorization.
5. Any attempt to add or reconfigure any College system, connecting a personal computer or other non-college computing device to the wired network, without written authorization from the CIO.
6. Running IT servers, whether virtual or physical, without the written authorization from the CIO.
7. Attempts to forge e-mail or other electronic information or any actions that degrade the accuracy of data.
8. Using College systems for any unlawful activity including but not limited to accessing child pornography, illegally downloading copyrighted material, or violating any license agreement or intellectual property rights in any way.
9. Using College systems to send spam, pranks, chain letters, pyramid schemes or other activities that negatively impact resources.
10. Using College systems in ways which violate College policy.

# Legal Standards

All users are expected to abide by all Federal, State and local laws. The following list is used for illustrative purposes, and is not intended to be a comprehensive guide:

1. FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.
2. GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.
3. HIPAA (Health Insurance Portability and Accountability Act): regulates the security and privacy of health information.
4. PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.
5. DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.
6. USC Title 18 §1030 (United States Code: Fraud and related activity in connection with computers)
7. **Unauthorized Use**

Violation of the regulations above is unethical and may constitute a criminal offense. Offenses may result in the suspension or permanent closing of usernames, campus disciplinary action, legal action, and/or other action.

Offenses will be dealt with according to any or all of the following: applicable Federal laws; Chapter 156 and 165.15 of the New York State Penal Law; the ACC Student Code of Conduct; other laws, regulations, employee contracts and handbooks, and policies of the campus, the State University of New York, the State of New York and the United States of America.