Corning Community College
Board Policy and Administrative Procedures

Policy Title:	Acceptable Use Policy	**RBOT Resolution #**	4161-16
Effective Date:	January 7, 2009	**Approval Date:**	
Issue/Amendment Date:	April 28th, 2016	**Author:**	Information Security Committee
Reference:	RBOT Policy Manual, Personnel Policies Handbook for Non-Union employees	**Rescinds**	#294409

1.0 Purpose

1.1 SUNY Corning Community College offers an extensive array of information resources to students, employees, and other members of the community. While the College's general policies and codes of conduct apply to any and all resources of the College, this Acceptable Use Policy further defines the special rights and responsibilities that apply to the use of the College's information resources.

The resources of the College include:

- All computers, equipment, software, networks, and related facilities owned, managed, or maintained by the College.
- The creation, processing, communication, distribution, storage, and disposal of information under the College's authority and span of control;
- All messages, data, files, programs, Internet web sites, and other material or information stored in or transmitted via the College’s systems.

Resources are made available to support and enhance the academic and administrative goals of the College. All persons authorized for access to these resources are referred to in this policy as “users.”

Each user shares in the responsibility to access resources appropriately and to protect such resources from unauthorized use.

2.0 Policy

2.1 It is the policy of Corning Community College (CCC) that all employees, Foundation, FSA personnel, students, contractors, affiliates, and other computer users are obligated to use these resources responsibly, professionally, ethically, and lawfully. College resources are provided to authorized individuals (i.e. students, employees, and affiliates) for the purpose of learning, teaching, and conducting business related to the operation of CCC. Using computing resources in any manner that violates any federal laws, New York State penal laws, State University of New York policies, or CCC policies and procedures is prohibited and may result in suspension or termination of computing privileges and/or suspension from the College.

2.2 User Acknowledgement. By logging into a College account, users agree to abide by and comply with all of the terms and conditions set forth in this policy. It is a user’s responsibility to read the policy and procedures carefully, prior to accessing College resources. Users are responsible for their unacceptable, unethical, or illegal use of college information technology resources.

3.0 Procedures

3.1 Authentication Requirements. CCC requires all employees, Foundation, students, contractors, affiliates, authorized guests, and other computer users to use their own unique login username and password to access computing resources. This identity verification process is to protect the individual's privacy. Individuals are responsible for maintaining their own secure password on College owned equipment and on personal devices that are used to access College files and/or data. Passwords are not to be shared with others. Upon approval of the Chief Information Officer or their designee, guests and consultants are issued a temporary password that expires upon completion of their visit.

User IDs and passwords are the primary method used to authenticate users prior to access to College resources. To ensure security of College resources, users must adhere to the following:

1. Access resources only from secure environments;
2. Change passwords regularly and never share passwords with others;
3. Use multi-factor authentication to access all services.
4. Report any perceived unauthorized access;
5. Notify the Information Technology (IT) department if passwords have been compromised;
6. Log out of sessions before leaving any resource unattended;
7. Safeguard resources from any threats to its accuracy or integrity;
8. Protect resources from unauthorized disclosures;
9. Cooperate fully during investigations of improper use.

Users may be held responsible for authorized or unauthorized activity conducted under their College issued ID.

No person, including any member of the IT staff, is authorized to request a user's password.

3.2 Authorized Use. Resources may be accessed and used only for the purposes authorized by the College. These purposes generally consist of work, professional development, study, research, service, or student activities consistent with the College's mission and goals. Authorized use of resources will comply with:

- Relevant College policies,
- State and federal laws and regulations,
- Third-party licensing agreements, and
- Intellectual-property rights, including copyrights.

The College acknowledges that limited personal use of its resources is compatible with a higher educational environment, but personal use will be incidental, at most, and may not cause the College to incur additional costs. In general, use must be appropriate and in compliance with College policies; not violate the law, licensing agreements or intellectual property rights; and not interfere with any individual's responsibilities.

3.3 Acceptable Use. Acceptable use standards require the following of each user:

1. To learn how to use College resources effectively and responsibly;
2. To accept responsibility for backup and security of their own work;
3. To abide by all security provisions;
4. To understand and respect software copyright laws;
5. To identify yourself clearly and accurately in electronic communication;
6. To respect the rights of others to have freedom from harassment or intimidation;
7. To recognize limitations to privacy in electronic communications.

3.4 Unacceptable Uses. Examples of unacceptable uses include, but are not limited to, the following:

1. Hack, tamper or attempt to gain unauthorized access to confidential information, obtain resources beyond their authorization;
2. Use resources in a malicious or harmful manner;
3. Use resources to threaten or harass any person or create a hostile place to work or study;
4. Intentionally degrade performance or deprive other users of access to resources;
5. Install software without the consent of IT;
6. Extend the network by introducing a hub, switch, router, firewall, wireless access point, server, or any other service or device without obtaining prior approval from IT;
7. Send unauthorized e-mail;
8. Use another user's account without permission;
9. Give or publish a password, identifying code or other confidential information of another user;
10. Attempt to corrupt or sabotage security systems or data protection schemes;
11. Engage in copyright infringement or other unauthorized downloading, copying and/or distribution of copyrighted material;
12. Engage in any illegal commerce or any illegal activity of any kind;
13. Use resources for personal gain, for the benefit of a third party, or for activities that are inconsistent with the College's tax-exempt status (such as political campaigning);
14. Store personal identifiable information such as social security numbers and College ID numbers on device hard drive or in any cloud computing space;
15. Create and/or operate websites on computers connected to the College network without obtaining prior approval from IT;
16. Attempt to destroy or sabotage the computer system or attempt to perform any act that impacts upon the proper operation of computer systems, such as intentionally spreading computer viruses;
17. Perform acts that waste computing resources or that unfairly monopolize resources to the exclusion of others such as excessive printing, sending chain letters, and sending unnecessary mass mailings.

All users of the computer system must act responsibly and maintain the integrity of the computer system. The College reserves the right to limit, restrict, revoke, suspend, or deny computing privileges and access to the computer system.

3.5 Security. To ensure security of resources users must adhere to the following:

3.5.1 Electronic Communications. All messages, data, files, programs, internet websites, and other material or information (individually and collectively referred to as "electronic communications") stored in or transmitted via the College's computer system are College records. Accordingly, the College reserves the right to access and disclose the content of electronic communications stored in or transmitted via its computer system:

1. as it deems appropriate for the administration and maintenance of the computer system;
2. when the College determines that such access or disclosure is necessary to investigate a possible breach of security, misuse of College resources, violation of law, or infringement of College rules;
3. when the College determines that such access and disclosure is necessary in connection with an academic, disciplinary, or administrative inquiry, or legal proceeding; or
4. for all other purposes permitted by law.

The College may routinely monitor and log usage data such as network session connection times and end-points, computer and disk utilization for each user, security audit trails, network loading, etc. Each user's use of the computer system constitutes consent to the College's access, disclosure, and monitoring. Users of the computer system should not have any expectation of privacy in any electronic communications stored in or transmitted via the College's computer system. Intellectual property rights for content of electronic communications are not governed by this Acceptable Use Policy.

3.5.2 Data Privacy. The College reserves the right to access, monitor, remove, and disclose any use of resources, or to block access to resources, without notice to users, after:

1. obtaining approval from an authorized College administrator, or,
2. receiving a court order or other legal demand, or,
3. determining that a compelling need exists to do so.

While the College diligently safeguards its resources, it cannot guarantee the security of resources against unauthorized access or disclosure. Users, therefore, should exercise extreme caution in using electronic messaging to communicate confidential or sensitive matters, and should not assume that their electronic messaging is private or confidential.

In addition, the College is subject to public records statutes that require us to make available records we maintain—both paper and electronic—for public inspection.

3.5.3 Remote Work. The use of an employee's personal computer to access work-related sites, applications, systems, and other information, is dependent on the use of appropriate security protocols. All employees must adhere to the following:

1. Under no circumstance may the employee allow college issued equipment to be used by any other person except as appropriate with their campus work obligation.
2. Use a Virtual Private Network (VPN) access to access Banner and Argos from remote locations.
3. Use multi-factor authentication to access all services.
4. Employees should log off and secure any computer being utilized to conduct official business when not in use, consistent with campus computer use policies.
5. Keep all applications and operating systems patched and updated with the latest supported releases.
6. Maintain up-to-date anti-virus software.
7. Safeguard all passwords used in connection with college files or programs and ensure sensitive information is protected.
8. Only take confidential information offsite when authorized in advance by their immediate supervisor/manager.
9. Protect and safeguard personal identifying information (PII**),** official records, information, files, documents, equipment, and other materials transported back and forth between the official work site and the alternate work site.
10. Avoid transferring or storing official data or information to any personal device or transfering work email to personal email addresses, text messaging , and social media services.
11. Do not share or make available any SUNY/campus information to other individuals except as appropriate and consistent with campus work obligation.
12. Comply with all established policies and procedures regarding protecting confidential and sensitive information. Securely store all hard copy documents or office media so that others cannot access it.
13. Do not communicate confidential information where others can listen.
14. Contact the Records Retention officer to properly dispose of confidential/sensitive documents requiring destruction.
15. Take appropriate action to protect the items from damage or theft. Loss or theft of equipment must immediately be reported to the remote worker's immediate supervisor/manager.

3.5.4 Unauthorized Access or Disclosure. Unauthorized access to or disclosure of official information or systems must be immediately reported to the immediate supervisor/manager and the Chief Information Officer, consistent with the SUNY Cyber Incident Reporting requirements. The employee must complete any required documentation of the suspected breach. Unauthorized access or disclosure, including the release of confidential information or personally identifiable information due to employee neglect, will be addressed through administrative actions.

4.0 Reporting Violations

4.1 Reporting. To report a violation of this policy, send an e-mail message to helpdesk@corning-cc.edu, or call the Helpdesk at (607) 962-9555.

4.2 Violators. The College reserves the right to limit, restrict, revoke, suspend, or deny privileges and access to College resources as it deems in its best interests, including:

- for the efficient and effective administration and maintenance of its resources;
- when necessary to investigate the possible breach of security, misuse of College resources, violation of law, or infringement of College rules;
- when required in connection with an academic, disciplinary, or administrative inquiry, or legal proceeding; or
- such other times or instances as permitted by law.

In order to enforce this policy and to comply with the enforcement of federal, state and local laws, IT may monitor, inspect, and retain contents of transmissions and files of College resources. If unauthorized use is found, IT will take immediate actions to remediate such abuse.

Violators of the Acceptable Use Policy are subject to the College's existing student or employee disciplinary procedures. Illegal acts involving College resources may also subject users to prosecution by local, state, or federal authorities.

In addition to these procedures, employees are responsible for adhering to the SUNY Information Security Policy (Document 6900).

5.0 Training and Review

5.1 Training. Employees shall complete annual training, which includes reviewing and acknowledging the review of the College's acceptable use policy.

5.2 Policy and Procedure Review. The College reserves the right to change this policy and procedures at any time. The Information Security Committee reviews the policy and procedures annually. The College will post updates and will inform users of such changes through College communications.

6.0 Definitions

6.1 Multi Factor Authentication (MFA). Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

6.2 Personal Identifying Information (PII). Per FTC guidance, PII is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

1. name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

2. unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. unique electronic identification number, address, or routing code; or
4. telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).”

6.3 Virtual Private Network (VPN). A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks

7.0 References

7.1 SUNY Information Security Guidelines: Campus Programs & Preserving Confidentiality #6608

7.1 SUNY Information Security Policy # 6900