Niagara County Community College

NCCCnet Computer Usage Policy

Document: NCCCnet Computer Usage Policy
Owner: Chief Information Officer
Version: 2.1
Revised August 6th, 2019

NCCCnet Use Policy

Introduction: Niagara County Community College (NCCC or College) provides computing resources to support NCCC users in academic research and the learning/teaching process.

Definitions:

1. NCCCnet means the College-provided, computer-based data systems which include, but are not limited to, the host computer systems, College-licensed software mobile devices, computers and related equipment, communication networks that specifically include, but are not limited to its local-area networks and virtual private networks that are either owned by the College or made available to the College under contract.

2. User means any NCCC student, College employee, or community member that uses or accesses NCCCnet.

3. Student means any person taking a credit bearing NCCC course.

4. College employee means any person being compensated by the College for services being provided in any capacity other than independent contractor.

5. Community member means any person who is not a NCCC student or College employee.

6. Electronic communications include, but are not limited to e-mail, voice mail, text messages, instant messages and information or content that is sent or received through NCCCnet (e.g., internet sites).

Confidentiality:

While unauthorized access of a User's NCCCnet account is prohibited, NCCC cannot guarantee confidentiality of any User's NCCCnet account. All data on a User's NCCCnet account and device is subject to review and disclosure. While it is not the normal practice of the College to monitor or limit access to content and use of NCCCnet, the College reserves the right to access and review information to assure the stability of the College's resources and to assure the User is not in violation of this or any other College policy. Users of NCCCnet have no expectation of privacy with regard to such use.

Software licensing:

Per U. S. Code, Title 17, Section 106, software shall only be distributed per the licensing software agreement. NCCC is obligated to enforce all software licensing agreements.

Software and Computer Hardware Allocation:

The Office of Information Technology will:

1.) Determine what software will be loaded onto NCCCnet.

2.) Assign all computing hardware and related equipment

3.) Users must obtain the approval of the Office of Information Technology for:

a. Moving any College-licensed software.
b. Moving any College-owned computing hardware or related equipment.
c. Loading any software onto NCCCnet.

Rights and Responsibilities of Users:

1) Only NCCC students and College employees are entitled to NCCCnet accounts. Proper college identification can be requested and must be provided to utilize college labs and/or college owned assets.

2) NCCCnet account is intended for the sole use of the assigned User, and is non-transferable.

3) Any time a User is accessing the college network or college resources, whether local or remote, the User must comply with the NCCCnet Use Policy.

4) All Users are responsible to respect the rights of other users.

5) All Users are expected to use NCCCnet in a responsible manner (e.g. Users should not consume unreasonable amounts of limited computing resources). Users are not permitted to download or install software on NCCCnet without the express permission of an authorized College official.

6) All Users are responsible to protect their NCCCnet account password from discovery or use by another person.

7) The assigned User is responsible for the usage of his/her NCCCnet account. If User knowingly or inadvertently makes his/her NCCCnet account password available to another person, he/she is responsible for any sanctions that may arise from the use of his/her NCCCnet account by another person.

8) All Users are responsible to report to the Office of Information Technology if they suspect that their NCCCnet account was accessed without permission.

9) All Users are responsible to change their NCCCnet account password if they suspect that their NCCCnet account was accessed without permission.

10) Users are responsible for backing up and recovering any data that is stored only on their electronic device (including those that are part of NCCCnet in order to assure the integrity of their data (see Rights and Responsibilities of NCCC for other stored data).

11) NCCC is not responsible for any privately-owned software, personal computers, cell phones, or related equipment brought by an employee, student or community member on College property, or used by an employee or student, for personal or College purposes.

Rights and Responsibilities of NCCC

1.) NCCC has the right to control all policies and procedures governing NCCCnet.

2.) NCCC has the right to monitor the use of all computing resources, and to protect the integrity of NCCCnet. NCCC reserves the right to monitor all communications transacted through NCCCnet. This includes, but is not limited to, mobile devices, telephone, and other network resources.

3.) NCCC has the right to monitor all software loaded onto NCCCnet and remove any unauthorized software.

4.) NCCC has the right to allocate the use of all NCCCnet resources (e.g., time, and space) as necessary. The Chief Information Officer has the discretion to allocate NCCCnet accounts.

5.) NCCC has the right to terminate any User's NCCCnet account.

   a. NCCC reserves the right to terminate employees' access to NCCCnet when their employee status ends.
   b. NCCC will terminate students' access to NCCCnet when their student status ends; either the student terminates enrollment or fails to enroll for the next consecutive semester.
   c. NCCC reserves the right to terminate any User's access to the NCCCnet if he/she violates this policy or he/she is no longer associated with NCCC.

6.) NCCC has the right to investigate any data stored on a User's NCCCnet account that caused or may cause a system problem and remove such data.

7.) NCCC will determine the level of access all Users have to data on NCCCnet.

8.) NCCC assumes no liability for loss of any data stored on a User's NCCCnet account due to system failure, User error or any other cause.

9.) NCCC has the right to monitor and log access to resources such as websites, email, and network shares as it relates to the standard business practice of the Office of Information Technology. If suspicious behavior is suggested or detected, the Chief Information Officer will coordinate with the supervising manager to provide detailed logging.

10.) NCCC is responsible for backing up and restoring any data that is stored on the file servers that support NCCCnet. NCCC will make best efforts to restore any files on such servers that become lost or corrupted, but cannot provide a guarantee that 100% of all such files will be recovered.

a. NCCC has the right to monitor the use of all computing resources and to protect the integrity of NCCCnet. NCCC will honor a User's right to privacy, but reserves the right to monitor all communications transacted through NCCCnet. This includes, but is not limited to, mobile devices, telephone, and other network resources.

Prohibited Behavior:
Prohibited behavior with respect to NCCCnet includes, but is not limited to any violation of law, College Policy and/or any of the following conduct:

1.) Violating any child pornography law, state or federal law, NCCC policy or software agreement.

2.) Copyrighted material is considered intellectual property of the owner. Any misuse of copyrighted material without the consent of the owner is illegal and punishable by law.

3.) Accessing or attempting to access an area of NCCCnet the User is not authorized to access.

4.) Disrupting or attempting to disrupt the integrity of NCCCnet.

5.) Altering or attempting to alter any College-licensed software or the configuration of any College-owned computer or related equipment.

6.) Circumventing or attempting to circumvent any data protection scheme.

7.) Discovering or attempting to discover any security loophole, or possessing software to do such.

8.) Decoding or attempting to decode any encrypted material.

9.) Deliberately wasting or overloading any NCCCnet resource.

10.) Viewing, downloading, trading or posting to an NCCCnet account or transporting across NCCCnet material that is non-business related, illegal, proprietary, obscene, in violation of NCCC contractual agreements, or otherwise damaging to NCCC. This includes, but is not limited to, the forwarding of chain email or other communications that cannot be considered business related.

11.) Harassing, threatening, defaming, or otherwise causing harm to another person whether by direct or indirect reference including sexual and racially offensive jokes.

12.) Accessing or attempting to access another User's NCCCnet account.

13.) Manipulating or attempting to manipulate data in another User's NCCCnet account.

14.) Sharing one's NCCCnet password and account with another person.

15.) Misrepresenting one's identity.

16.) Plagiarizing any work (e.g. text, graphics or programs).

17.) Violating any software agreement.

18.) Using NCCCnet for any commercial purpose unless authorized by the Office of the President.

19.) Reading, deleting, copying, or altering communications of others.

20.) Sending unsolicited for profit personal messages or chain letters.

21.) Employees using the internet and e-mail, during or outside of normal working hours, for other than authorized NCCC educational or NCCC work related purposes.

22.) Permitting persons not considered to be Users (per this policy) access to equipment reserved for College Users.

23.) Installation or alteration of wiring, including attempts to create network connections, or any extension or retransmission of any NCCCnet services or content without the approval of the Office of Information Technology.

24.) Reselling of services based on the use of NCCCnet. This includes, but is not limited to, web server space, email, and use of lab equipment.

Any of these behaviors by a User will prompt a College official to take action.

Any communications or complaints regarding a potential violation of the NCCCnet Use Policy or misuse of NCCCnet resources should be directed as follows (based on the classification of the User):

Student:
Suspected violation should be reported to the Vice President of Student Services, or designee, and handled through the Student Code of Conduct Policy.

While investigating the suspected violation or misuse, the Vice President of Student Services, or designee, may suspend a student's NCCCnet privileges. The Office of Student Services will notify the student, in writing, within three (3) working days that his/her NCCCnet privileges were suspended.

Employee:

The suspected violation should be reported to the Director of Human Resources, or designee, and handled in accordance with College employee policies and collective bargaining agreements. Any employee determined to be in violation of this Policy shall be subject to administrative and/or disciplinary action, up to and including termination from employment.

Community Member:

The suspected violation should be reported to the Chief Information Officer, or designee, in accordance with the College's Information Security policies and other pertinent practices/procedures of the Security Department.

Any suspected violation that could constitute a potential breach of information security should be immediately reported by the above individuals (as applicable) to the Chief Information Officer in accordance with the College's Information Security Policy.

Sanctions:

User's NCCCnet privileges may be suspended if the suspected violation is reasonably perceived to constitute unlawful activity, pose a risk to the integrity of NCCCnet, or present a threat to the safety or welfare of NCCC, a student, College employee, or another person in the community. Penalties that may be imposed include, but are not limited to reprimand, temporary or permanent loss of using NCCCnet, or referral to College, State and/or Federal authorities, in addition to the penalties and consequences otherwise set forth above with regard to Prohibited Behavior.

Interpretation and Revision:

Any question about the NCCCnet Use Policy shall be referred to the Chief Information Officer for explanation or interpretation.

The NCCCnet Use Policy shall be reviewed annually.