NCC Computer Systems & Information Use Policy

October 16, 2018

Submitted by:

Michael Oldenkamp

Director, Technology and Information Services

Technology Planning Committee

Contents:

Article I.	Introduction	3
Article II.	Policy Statements	4
Article III.	Policy Administration	5
Article IV.	Management Responsibility	6
Article V.	Data Ownership	6
Article VI.	Electronic Mail & Internet Use	7
Article VII.	Security	7
Article VIII.	Computer Application Development Controls	10
Article IX.	NCC Computer Systems & Information Use Agreement	11
Article X.	Social Media Use Policy	12

Article I. Introduction

Northwest Iowa Community College (NCC) has committed to improving its use of information technology to increase productivity, maximize operating capabilities and efficiencies providing our customers a useful and secure environment to support their learning endeavors. This commitment brings tremendous benefits, but also introduces new administrative concerns and responsibilities. Namely, NCC's information must be protected from natural and human hazards, and every authorized user of NCC's systems must follow established practices to ensure that these hazards are minimized and/or their effects minimized. This Computer Systems & Information Use Policy ("Policy") addresses these purposes by:

(a) Physically protecting information processing facilities and equipment. This includes securing mobile devices such as laptops, tablets and phones in safe locations when not in its presence (store your device in your trunk if you have to leave it in your car).

(b) Maintaining application and data integrity.

(c) Ensuring that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.

(d) Protecting against unauthorized disclosure of information.

(e) Assuring the continued availability of reliable and critical information.

Many of NCC's program operations are fully dependent upon automated information services to perform or support daily functions. This Policy strives to eliminate or minimize the effects of risks relative to interruption, disruption, or loss of these information support services.

Information managed by automated information systems must be protected from errors, misuse, unauthorized or accidental modification, destruction, and disclosure.

An effective information resources program requires active support and ongoing participation from many people. Implementing cost-effective security practices will minimize or eliminate the vulnerabilities associated with a large group of users.

User awareness is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of information resources. This Policy identifies the means for protecting these resources and defines the security and data ownership responsibilities of the information resources that are maintained and operated by NCC's Technology & Information Services Department. This Policy should be used to conduct periodic reviews of security awareness.

The NCC Computer Systems & Information Use Policy applies to all NCC Users including Staff, Faculty, Students, and others authorized to access applications and computer systems operated by NCC's Technology & Information Services Department.

Article II. Policy Statements

Section 2.01 Principles

(a) Information resources (including but not limited to computer hardware and software) are the property of NCC and shall be protected as such. Information resources may be used only for **College Purposes**. Information resources are valuable assets - unauthorized use, alteration, destruction, or disclosure of these assets is a violation of this Policy.

(i) **College Purposes**: For purposes of this policy, "**College Purposes"** refers to all communications, file creation, information storage, and similar matters involved in conducting the business of the College, i.e., in providing education to and for students and in providing educational and administrative support.

(ii) Private or personal use for profit is prohibited. Private or personal use not for profit is allowable under the provisions of this document as long as this type of use does not interfere with **College Purposes**.

(iii) All users have the responsibility to use these resources in a professional, ethical, and lawful manner.

(iv) Student network storage space (H drive) will be limited to 2 GB per user.

(b) Attempting to circumvent security or administrative access controls for information resources is a violation of this Policy. Assisting someone else or requesting that someone else circumvent security or administrative access controls is also a violation of this Policy.

(c) Persons granted user IDs to access information resources will be required to abide by this policy when logon IDs and passwords are assigned.

(d) Violations of the NCC Computer Systems & Information Use Policy will be reported to NCC's Director of Technology and Information Services and other appropriate personnel.

Section 2.02 Practices

(a) All persons are required to review, understand and agree to comply with the NCC Computer Systems & Information Use Policy upon access being granted.

(b) Logon IDs and passwords must control access to all information resources. The logon ID owner is responsible for managing his/her password according to the guidelines specified in this policy.

(c) **Confidential Information** shall be accessible only by authorized personnel. Data containing any **Confidential Information** shall be readily identifiable and treated as confidential in its entirety. When **Confidential Information** from a department is received by another department in the connection with the transaction of NCC business, the receiving department shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing department.

(i) **Confidential Information:** For purposes of this Policy, **"Confidential Information"** refers to data and other information, the unauthorized disclosure of which could be prejudicial to the College or could be a violation of any State or Federal privacy laws.

(d) Anyone accessing an application must receive appropriate training for using the application and must acknowledge the security and privacy requirements for the data contained in the application. Personnel security and security awareness contains additional information.

(e) When an employee terminates employment, his/her access to information resources will be terminated. Non-employee user accounts will be terminated when they are no longer required. Student accounts will remain active for students enrolled in the current or upcoming term. All other student accounts will be active for a period of three months following the last term enrolled. Adjunct faculty accounts will be disabled after one year from the starting date of the last term employed as an instructor. Accounts will be deleted after one year of being disabled.

(f) Computer end-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system (i.e. privacy screens, etc.).

(g) All computer end-user workstations will have virus protection software installed. Removal of this software is a violation of this Policy unless approved by the Technology & Information Services Department.

(h) All information processing areas used to house information resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel. This includes all system servers and associated equipment.

(i) Individuals who experience computer-generated threats or harassment should immediately report the incident to Title IX Equity Coordinator (Brandi Hansen for employees, bhansen@nwicc.edu, or Beth Frankenstein, bfrankenstein@nwicc.edu for students).

(j) All development staff for mission critical applications are required to adhere to security guidelines contained in Computer Application Development Controls.

(k) Persons violating the Computer Systems & Information Use Policy will be subject to appropriate disciplinary action, up to and including termination or expulsion.

Article III. Policy Administration

NCC's Director of Technology and Information Services administers the Computer Systems & Information Use Policy. This person is responsible for:

(a) Monitoring computer security issues.
(b) Filing reports on computer security issues.
(c) Keeping users aware of computer security issues.
(d) Monitoring compliance with this Policy.
(e) Conducting audits as directed by NCC management.

Article IV. Management Responsibility

Each supervisor is responsible for the security access of information in all facilities under his/her jurisdiction and for implementing information security requirements for the supervisor's area of responsibility.

Article V. Data Ownership

For purposes of this Policy, data is owned by the College department primarily responsible for creating and maintaining data content. *(Notwithstanding the foregoing, such ownership remains subject to the oversight and ultimate control of the College via the College's president and his or her designated personnel.)* Data is not owned by individuals who develop or maintain the data. College department employees are responsible for the data created, maintained, and used by their department. These employees are required to follow Data Owner Responsibilities.

Section 5.01 Data Owner Responsibilities

The data owner is primarily responsible for:

(a) Maintaining information in the data file.
(b) Determining how the data should be used.
(c) Authorizing who may access the data.

Section 5.02 Data Custodian Responsibilities

The data custodian is the group or individual(s) assigned to supply services associated with the data. The custodian is:

(a) The Technology and Information Services department for centrally supported applications.
(b) The operator of a departmental computer system, server, or network of computer workstations.
(c) The data custodian provides services in accordance with the directions from the owner or other authorized person and is responsible for:
  (i) Implementing and/following owner-specified controls over the data.
  (ii) Providing security controls for access to systems.
  (iii) Insuring that users comply with security procedures.

Section 5.03 Data User Responsibilities

The data user is the person who has been granted authorization to access the data. This authorization must be granted according to established procedures. The user must:

a) Use the data only for authorized **College Purposes**.

b) Comply with security measures specified by the owner or custodian.

c) Not disclose information in the data nor the access controls over the data unless specifically authorized.

Article VI. Electronic Mail & Internet Use

NCC provides electronic mail (email) and access to the Internet as part of the college's information resources. Its purpose is to allow persons to communicate and research within the guidelines of this policy.

The information in email messages and files and Internet use is subject to disclosure to NCC management without notice to the individual. It is *not* private to the individual user.

All computer e-mail and Internet users have the responsibility to use these resources in a professional, ethical, and lawful manner. Some examples of prohibited use include but are not limited to: exchanging or saving material that may be considered pornographic or obscene; jokes that are demeaning or may be considered offensive; any message/College-administered social media post that may be considered demeaning, defamatory or discriminatory. Such uses may constitute a violation of this policy, NCC's harassment policy or other policies and could result in disciplinary action up to and including expulsion or termination.

E-mail groups such as All Users; All Students; All Staff & All Faculty are not to be used for personal use.

Personal email for profit is prohibited. All other personal email that is excessive and/or interferes with College Purposes is also prohibited.

Archival/storage of old messages
Every email message sent or received through NCC's email system is archived for a period of 2 years. Emails older than 2 years are deleted from the archive system.

Email will be deleted from the email servers automatically according to these guidelines:

Student:
- Inbox – 180 days
- Sent Items – 180 days
- Junk Email folder – 30 days
- Deleted Items – 30 days

Employees:
- Sent Items – 180 days
- Junk Email folder – 30 days
- Deleted Items – 30 days

Article VII. Security

All computer systems will require a user ID and password for access. You are responsible for any/all activity that takes place under your user ID. Do not leave your computer unattended without locking it down (ctrl – alt – delete – lock computer) or logging off. Group policies are enforced that automatically lock an NCC computer that has been idle for 10 minutes. Do not share passwords with other people or allow others to use your logon. Group policies are enforced that lock out a user for failing to enter the correct credentials 5 times. Users that have a locked account will have to contact the IT department to unlock their account.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of inappropriate activity, system personnel may provide the evidence of such monitoring to NCC executive management.

Persons violating the Computer Systems & Information Use Policy will be subject to appropriate disciplinary action, up to and including termination or expulsion.

Section 7.01 Personnel Security and Security Awareness

In any organization, people are the best tool in maintaining effective security. At the same time, people represent the greatest threats to information security. No security program can be effective without awareness and motivation.

(a) Requirements

Everyone is responsible for systems security to the degree that they require the use of information and associated systems. Fulfillment of security responsibilities is mandatory and violations of security requirements may be cause for disciplinary action including termination or expulsion.

(b) Security Awareness and Training

An effective level of awareness and training is essential to a viable information security program. Individuals who are not informed of risks or of management's policies and interest in security are not likely to take steps to prevent the occurrence of violations. Data owners should provide periodic awareness discussions about information security and the protection of information resources.

(c) Acknowledgment of Rights and Responsibilities

Individuals with access to application systems acknowledge the security requirements of the systems and their responsibility to maintain the security of the systems before access to the system is granted. All users, by accessing college resources, acknowledge agreement to comply with the stipulations identified in this Policy.

(d) Termination Procedures

Upon termination or dismissal of a person who occupies a position of special trust or responsibility, or has access in sensitive areas, management will revoke all access authorizations to information resources.

Section 7.02 Password Management

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure and destruction. Effective controls for access to information resources minimizes error and negligence, and reduces opportunities for computer crime. Each user of an automated system (e-mail, network drives, student information system, etc.) is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access.

Section 7.03 Password Selection Advice

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is ineffective, compromising security and accountability of actions taken by the logon ID that represents the user's identity. Therefore, any password that somebody else might guess to be a password is a bad choice.

What are bad passwords? Your name, spouse's name, or parents' names are easy to guess. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad; because there are fewer digits, they are more easily guessed. Especially bad are "magic words" from computer games, such a XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some tips for choosing a good password are:

(a) Include digits as well as letters (combine upper and lower case). Special characters are helpful as well if the system supports them in the password.
(b) Choose something easily remembered so it doesn't have to be written down.
(c) Use at least 8 characters. Password security is improved slightly by having long passwords.
(d) Your password should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.

Section 7.04 Password Handling Advice

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, on a Post-It label attached to your computer terminal, or on the pullout drawer of your desk.

A password you memorize is more secure than the same password written down, simply because there is less opportunity for other people to learn it. But a password that must be written down in order to be remembered is quite likely a password that is not going to be guessed easily. If you write a password and keep it in your wallet, the chances of somebody who steals your wallet using the password to break into your computer account are remote.

Password Database Utilities may be used to safely store passwords in an encrypted database. Examples of utilities include PassWordSafe and KeepPass.

If you must write down a password, follow a few precautions:

(a) Do not identify the password as being a password.
(b) Do not include the name of the account or the computer on the same piece of paper.
(c) Do not attach the password to a terminal, keyboard, or any part of a computer.
(d) Mix in some "noise" characters or scramble the written version of the password in a way that you remember, but make the written version different from the real password.
(e) Never record a password on-line and never send a password to another person via electronic mail.

This information on passwords was adapted from the book Practical UNIX Security by Simson Garfinkel and Gene Spafford.

Article VIII. Computer Application Development Controls

All computer applications development staff and contractors are required to adhere to the following security guidelines. Responsibility for compliance applies to Managers, Analysts, Contractors and Programmers:

(a) Systems and programs must perform only the functions requested and may not cross over into other systems except as specified.

(b) System development resources such as terminals, computers, and development software may be used only for approved projects.

(c) Change logs will be maintained and will include information for each change that identifies: requester, action taken, by whom, date, and approval authority.

(d) Modifications must be approved by the development management and management of the organization that "owns" the application system. Student Information Systems access must be approved by the department's supervisor.

(e) Unauthorized changes to production systems are not allowed and are considered violations of the NCC Computer Security Policy.

(f) Procedures are required which include adequate testing prior to implementation, security against modification of production data, controlled access to data, production, and program libraries.

(g) Managers will convene system review, inspection, and walk-through meetings periodically to insure adherence to these controls and to insure the general state of computer security.

(h) Managers will solicit and/or provide effective security training for all staff engaged in application development.

(i) Security procedures, work practices, programming methods, standards, production libraries, and overall data security will be subject to review by the Computer Security Auditor.

(j) Only the Production Control staff should perform running programs that update production databases.

(k) Production Control staff should only have read-only access to production program libraries and should not have access to program source code libraries.

(l) Movement of programs and source code libraries into production must be approved by appointed application administrators.

(m) All change requests and problem reports must be in written form in the helpdesk system and have the approval of authorized representatives.

(n) All new database structures and changes to existing database structures must be approved by the Database System Administrator before the modified structures are put into production.

A periodic review and report of all uses of a super-user password will be conducted.

Article IX. NCC Computer Systems & Information Use Agreement

Section 9.01 Adherence to NCC Computer Systems & Information Use Policy

NCC recognizes that information and information systems are critical and important assets. NCC will take appropriate steps to protect information and information systems from a variety of threats such as error, fraud, sabotage, privacy violation, and service interruption. This Policy provides direction of consistent and standard access controls across platforms and applications to protect information and information resources. This Policy applies to all NCC resources regardless of physical location. This Policy will be updated periodically based on technology standards with input and approval from NCC management.

Section 9.02 Disclosure of Automated Information – Confidentiality

The user hereby acknowledges that in and as a result of performing services for Northwest Iowa Community College, the user will be making use of, acquiring and/or adding to automated information and resources having a special and unique nature and value relating to NCC. This shall include but not be limited to computerized data systems, systems software and the use of associated equipment and information that is the property of NCC, their clients or external vendors.
Information includes but is not limited to information related to design, programming techniques, security techniques, flow charts, student lists, supplier information, source code, object code, proprietary software, documentation or any other data.
The user further acknowledges that the disclosure of such information could cause a substantial decrease in the value of NCC's business or result in legal action by the owner of the information. The ability to access such information is being given only because of the position of confidence and trust the user will occupy as an NCC agent.

Section 9.03 General Conditions

The user agrees that he/she will not, at any time, during or following the term of his/her access, directly or indirectly disclose, publish, divulge, or use (except in connection with the provision of services) any such information obtained by or disclosed to him/her through or in the course of his/her association with NCC. By accessing the college's resources, the user agrees that his/her obligations shall include:

(a) Using his/her best efforts to prevent disclosure of assigned access codes or passwords.
(b) Immediately informing Management if he/she becomes aware of any other persons obtaining knowledge of any access codes or passwords they are not authorized to use.
(c) Immediately informing the appropriate NCC people if he/she becomes aware of any other persons misusing information.
(d) Upon termination or dismissal for any reason, the user shall immediately return to NCC any and all confidential documents or information relating to NCC, clients or external vendors of automated systems or information.
(e) Compliance with the NCC Computer Systems & Information Use Policy.

Section 9.04 Philosophy

The user recognizes his/her responsibility to manage and to work in a manner that supports NCC's Mission Statement.

Section 9.05 Written Modification

There shall be no modification of this Agreement, except in writing and executed with the same formalities as this Agreement.

Section 9.06 Violations

Persons violating the NCC Computer Systems & Information Use Policy will be subject to appropriate disciplinary action up to and including termination or expulsion. Such actions do include but are not limited to breaking copyright laws, illegal downloading of music, private "for profit" use, pornography, or any activity that is offensive.

Section 9.07 Agreement to Comply:

By accessing college resources, the user agrees to have read, understood and agree to all provisions identified in the NCC Computer Systems & Information Use Policy.

Article X. Northwest Iowa Community College's Social Media Policy

NCC maintains an official presence on several popular social media sites including Facebook, Twitter, and LinkedIn. NCC supports employees using social networking websites, blogs, micro-blogs, and other online media ("Social Media") to promote the College.

Using Social Media

Section 10.01 Plan ahead
If you want to use social media in connection with your work for NCC, it's a good idea to think in advance about how you will use social media to achieve your department's objectives. Develop a plan that addresses such issues as how frequently you will review and update content, and monitor and respond to comments from visitors to your site. It is recommended to post three times a week, but you must post at least once a week. It is recommended that you either have a separate social media account for NCC purposes, or do not use social media accounts for personal posts that are associated with your NCC email.

Section 10.02 Get off to the right start
Departments should designate a social media account administrator who will be responsible for the social media site. To set up an official NCC social media site the proposed account administrator must seek approval from the Marketing Department staff. All social media accounts must include Marketing Department staff as administrators. If there is only administrator allowed by the social media site the username and password must be provided to the Marketing Department to keep on file. Coordinate with the Marketing Department staff to learn what the best practices are for your chosen social media platform prior to starting any social media site. Contact the Marketing department at marketing@nwicc.edu for more information.

Section 10.03 Follow the rules
Social media websites have terms and conditions that users must follow in order to use the sites. You should read, understand, and follow those rules. Also, remember that NCC policies, such as the Computer

Use Agreement (available at http://www.nwicc.edu/Post/sections/371/Files/NCC_Computer_Systems-Information_Use_Policy.pdf) apply to your use of social media as an employee.

Section 10.04 Be honest about who you are
If you are promoting Northwest Iowa Community College and its programs and activities be honest about your identity and affiliation with the College. Do not hide or misrepresent your identity if you are posting on behalf of NCC.

Section 10.05 Be accurate and correct mistakes
Have the correct information about programs and events before you post. If you make an error acknowledge your error and correct it as quickly as possible. Depending on the platform, you can edit your post or just delete the post and start over if no one has commented on it. It is ok to say you need some time to find the correct answer.

Section 10.06 Always answer questions from your social media site promptly
Best practice is to respond within hours of the post, but no longer than 24 hours. Even if you do not know the answer you can say, "Great question, _____. Let me look into that and I will get back to you later today". You MUST get back to them within the stated time! Even if that is to say you are still looking into the matter.

Section 10.07 Develop and maintain your presence
Post news, events, and information that is relevant to your target audience. You may find that it's a process to develop the right "online voice" for your audience. Don't be reluctant to change course if you are not achieving your goals.

Cross-promote your social media presence in other channels/materials to drive traffic to your social media site and vice versa. The Marketing Department staff can tell you what the best practices are for each social media platform. While your department's use of social media will depend upon a number of factors once you establish a social media presence, parents, students, and others will find you and expect to engage with you via social media.

Establishing a social media presence that you do not maintain will reflect poorly on your department and NCC. It is recommended that you post at least three times a week, but you must post at least once a week.

Section 10.08 Be professional (think before you post)
For employees using social media as part of their jobs the same good judgment, common sense, and discretion that apply to using more traditional forms of communication should be followed. On social media, employees should be guided by an even heightened concern for protecting their own reputations, the reputations of others, and the reputation of the College. Online posts are permanent and responses to the post are uncontrollable. Try to be mindful at all times that you are representing NCC when you post or comment on a site. If you have questions or concerns about whether it is appropriate to post certain material speak with the Marketing Department staff before you post.

Section 10.09 Have a plan for responding to negative comments
If an online commenter posts an inaccurate, accusatory, or negative comment about NCC on your NCC social media site, feel free to correct the inaccuracy but do so in a positive and polite way. Do not get into a lengthy negative discussion (more than three posts). If you find yourself in a position where the

communications become lengthy (more than three comments) antagonistic or deal with sensitive topics, ask the Marketing Department staff for advice before responding.

It is NCC's policy only to remove comments that directly attack someone, threaten someone, or use profanity. Social media is a communication tool. At times there may be negative comments. The goal is through the use of communication to work through issues and accommodate all parties.

If you see negative comments posted online about NCC please bring them to the attention the marketing department staff to learn what the best practices are for your chosen social media platform prior to starting any social media site. Contact the Marketing department at marketing@nwicc.edu for more information. While online comments about NCC are monitored it is always nice to have extra eyes looking out for NCC's best interests. There is an online response team who discusses online comments and if it is appropriate for the College to respond. This team is made up of: the President, the Vice President - Institutional Advancement & External Affairs, and the Director of Marketing & Communications. In many cases the most appropriate thing to do is not respond and monitor the site.

Section 10.10 Maintain confidentiality and respect copyright law
Do not discuss confidential or sensitive internal issues online. Some situations are better handled through a personal message or ask the commenter to call you directly. Be conscious of the laws and regulations governing the privacy of student education records (FERPA), protected health information (HIPAA), personally identifiable information, and private information about colleagues. Do not post confidential information about faculty, students, alumni, or other employees.

Also be mindful of copyright and trademark protections that may limit what materials you may use online, including photos and music. Most trademarked music is not allowed on social media and the use of it can lead to your account being closed by the social media site itself. Contact the Marketing Department staff with any questions.

Maintaining the security of your social media profile can be a complicated and ever-changing effort. Educate yourself on the security issues and options on your chosen social media outlet and set up your profile appropriately. Be aware that social media outlets can—and frequently do—change their privacy policies. So something that may have been private on your profile yesterday may not be protected tomorrow.

Section 10.11 Escalated/Serious Issues
If you identify issues related to health, safety, or security while using social media, bring them to the attention of the appropriate resource at NCC immediately. Information security issues should be addressed to the IT department (it@nwicc.edu). If you become aware of material online that prompts concerns about student health or safety you should refer to the Emergency Action Plan for the appropriate response.

Section 10.12 Account Administrators
All social media accounts officially recognized by NCC must have a NCC faculty or staff member as an administrator at all times. The Marketing Department staff must have administrator access to all official accounts.

Should a social media account administrator leave the employment of NCC or if they no longer wish to be an account administrator a new account administrator must be appointed before the employee leaves or

discontinues account administrator duties. It is the current account administrator's responsibility to designate another NCC employee to be an account administrator prior to being removed from that role. When a new account administrator is identified or if a new account administrator cannot be identified the Marketing Department staff should be notified immediately.

NCC employees identified as account administrators are held responsible for managing and monitoring content of their officially recognized accounts. Account administrators are responsible for removing content that may violate NCC's policies. If the post contains a direct or indirect threat to an individual or the College, please refer to the Emergency Action Plan for the appropriate response. It is required that you take a screen shot of the post before you delete it. NCC is not liable for any social media activities of its employees or actions resulting from social media use of NCC employees.

In the event that an account is determined by the Marketing Department staff to be inactive, ineffective, or inappropriate, the Marketing Department staff will meet with the account administrator(s) to rectify the situation. If the issue is not resolved, the Marketing Department staff is authorized to close the account and remove it from public access.

Section 10.13 Using Social Media for Your Own Purposes

When using social media for yourself consider the privacy issues involved. Although some websites have privacy settings you cannot rely on such settings to guarantee your online information and postings will be kept private. Many social media sites are continuing to develop their security features, but even the best information security features can be compromised. Before you post, consider that you will potentially be sharing it with an audience of millions.

If you identify yourself as an employee of Northwest Iowa Community College on your website or blog you must state that you are sharing your views as an individual, not as an official representative of NCC. For example, include a disclaimer on your website or blog that states: "The views expressed on this [blog/website] are mine alone and do not necessarily reflect the views of Northwest Iowa Community College."