NCC Computer Systems & Information Use Agreement
Updated: July 20, 2025

Submitted by:
Michael Oldenkamp
Director, Technology and Information Services

Technology Planning Workgroup

Contents:

- Introduction
- Agreement Statements
- Agreement Administration
- Management Responsibility
- Data Ownership
- Electronic Mail & Internet Use
- Security
- Computer Application Development Controls
- NCC Computer Systems & Information Use Agreement
- Social Media Use Policy

Introduction

Northwest Iowa Community College (NCC) is committed to maintaining a secure, efficient, and user-friendly computing environment. As technology evolves, so do the risks associated with information security. This updated agreement outlines the best practices and responsibilities for all authorized users of NCC's computing systems.

Agreement Statements

- All persons are required to review, understand and agree to comply with the NCC Computer Systems & Information Use Agreement upon access being granted.
- NCC's information resources (hardware, software, data, and networks) are the property of the institution and should be used exclusively for College Purposes.
- Personal use of NCC resources must not interfere with college operations. Any unauthorized use, alteration, destruction, or disclosure is a violation of this agreement.
- Attempts to circumvent security measures or unauthorized access will result in disciplinary action.
- Student network storage (H drive) will be limited to **2 GB per user.**
- Persons violating the Computer Systems & Information Use Agreement will be subject to appropriate disciplinary action, up to and including termination or expulsion.
- User awareness is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of information resources. This Agreement 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 Agreement should be used to conduct periodic reviews of security awareness.

- 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 agreement
- 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.
- Confidential Information: For purposes of this Agreement, "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.
- 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.
- 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.).
- All computer end-user workstations will have virus protection software installed. Removal of this software is a violation of this Agreement unless approved by the Technology & Information Services Department.
- 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.

Agreement Administration

The Director of Technology and Information Services oversees compliance, security monitoring, and periodic audits.

Management Responsibility

Supervisors must enforce security access controls and ensure compliance within their respective areas.

Data Ownership

- Data is owned by the department responsible for its creation and maintenance.
- Confidential data must be accessible only by authorized personnel.
- Data custodians must implement proper security controls to protect institutional data.

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 agreement.
- NCC email is archived for **two years.**
- Email and internet activity are monitored and subject to disclosure to NCC management.
- Prohibited activities include sharing offensive content, unauthorized file downloads, and using email for profit.
- Multi-factor authentication (MFA) is now required for all employee NCC email accounts while accessing from off-campus.
- Email retention policy:

    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

Security

- Workstations must be locked when unattended (auto-lock enforced after **10 minutes** of inactivity.
- Users must change passwords **every 365 days**.
- Passwords must contain **12 characters**.
- IT will conduct quarterly security awareness training sessions through the KnowBe4 training platform.

Computer Application Development Controls

- Unauthorized changes to production environments are strictly prohibited.
- 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 Agreement.

- 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.

NCC Computer Systems & Information Use Agreement

- Users must acknowledge this agreement before being granted access.
- Violations may result in disciplinary action, including termination or expulsion.

Social Media Use 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.

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.

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.

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 procedures, such as the **NCC Computer Systems & Information Use Agreement** apply to your use of social media as an employee.

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.

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.

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.

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.

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.

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 Creative Services Coordinator, the Digital Media Specialist, and the Director of Marketing & Communications. In many cases the most appropriate thing to do is not respond and monitor the site.

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.

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 marketing department (marketing@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.

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 and must notify the marketing department. 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.

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.”

Conclusion

This agreement is designed to safeguard NCC’s technology resources while ensuring they remain accessible and useful for the college community. Regular updates will be made to adapt to emerging technological challenges and security concerns.