COMMUNITY COLLEGE SYSTEM OF NEW HAMPSHIRE

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Information Technology Acceptable Use	Date Approved: June 16, 2009
Policy #: 321.01	Date of Last Amendment: January 6, 2010
Approved: Richard A. Gustafson, Chancellor	Effective Date: July 1, 2009

321.01 INFORMATION TECHNOLOGY ACCEPTABLE USE

1. Purpose:

The purpose of this policy is to encourage the responsible use of CCSNH and member campus technology resources consistent with expectations for the appropriate conduct of the members of our campus communities. This policy is intended to provide guidance to CCSNH technology users. While this policy and Addendum-A (Examples of Violations) are intended to provide guidance, it is impossible to contemplate all potential applications since technology and applications consistently change. If unsure whether any use or action would constitute a violation of this policy, contact your campus Information Technology department or the System Office for assistance. In cases not covered explicitly by the CCSNH Acceptable Use policy, the System Office determination will prevail**.** In addition to this policy, information on how to use CCSNH technology, resources and services can be found at www.ccsnh.edu

Access to CCSNH technology resources is a privilege, not a right. This privilege is extended to all users including faculty, staff, students, alumni/ae, and affiliated individuals and organizations. CCSNH's technology resources include computing facilities, telecommunications and network services, video network services, web page servers, equipment, software, applications, information resources, printing and scanning services, and user and technical support provided by Information Technology staff. Accepting access to these technology resources carries an associated expectation of responsible and acceptable use. Failure to abide by the responsibilities articulated below may result in loss of privileges.

2. Responsibilities

Users of CCSNH technology resources have a shared responsibility with our Information Technology staff to maintain the integrity of our systems, services, and information so that high quality and secure services can be provided to everyone. Toward this end, all users shall:

a. Comply with posted policies governing use of computing and printing facilities.

b. Respect all contractual and license agreements, privacy of information, and the intellectual property of others.

c. Comply with federal, state, and local regulations regarding access and use of information resources (e.g., policies regarding Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, codes of professional conduct and responsibility, etc.).

d. Maintain and secure your own system accounts (including files and data associated with those accounts); this includes taking action to backup your files and data as appropriate.

e. Exercise due diligence in protecting any computer you use to connect (either through dial-up, VPN or any other means) to the CCSNH network from viruses, worms, and security vulnerabilities by maintaining and regularly using anti-virus software, installing available security updates/patches for your operating system and any applications you use, and avoiding the installation of un-trusted programs on your computer.

f. Take precautions to keep your technology accounts (computer, network, Blackboard, Banner, etc.) secure.

g. Do not share privileges with others. Your access to technology resources is not transferable to other members of the CCSNH community, to family members, or to outside individuals or organizations. If someone wishes access to CCSNH's technology resources, s/he should contact the CCSNH Information Technology Office by sending email to ITSupport@ccsnh.edu

h. Ensure that any and all of your web pages and blogs reflect the highest standards of quality and responsibility. As page or blog owner, you are responsible both for the content of your web page or blog and for ensuring that all links and references from these are consistent with this and other policies, copyright laws, and applicable local, state, federal laws. CCSNH hosted web pages and blogs are not to be used for commercial purposes or for activities unrelated to the educational mission of the college without written authorization from the CCSNH.

i. Ensure that any contributions of information to WIKIS reflect the highest standards of quality, accuracy, and responsibility.

j. Understand the implications of sharing information or data via the Internet, e-mail, Instant Messaging, social networks or other services that are either open to access by others, or that can be viewed and/or forwarded to others.

k. Report violations or suspected violations of this policy. Please report violations as follows:

- College Personnel: Report violations to your immediate supervisor, Vice-President of Academic Affairs or President.
- System Office Personnel: Report violations to your immediate supervisor, Vice-Chancellor or Chancellor.
- Students: Report violations to your College Vice-President of Academic Affairs or President.

3. Enforcement of this Policy

CCSNH reserves the right to monitor the System network and systems attached to it, and to take actions to protect the security of the CCSNH systems, information, and users.

a. Reporting Violations or Suspected Violations: Reports of violations or suspected violations as follows:
    1. College Personnel: Report violations to your immediate supervisor, Vice-President of Academic Affairs or President.
    1. System Office Personnel: Report violations to your immediate supervisor, Vice-Chancellor or Chancellor.
    2. Students: Report violations to your College Vice-President of Academic Affairs or President.

b. Response to Violations: The CCSNH Information Technology office will investigate and respond to reports of violations or suspected violations and include appropriate CCSNH offices as necessary. As part of this response, Information Technology reserves the right to immediately disconnect any system or terminate user access to protect the security of the CCSNH systems, information, and users.

c. Sanctions: Violation of this policy may result in the immediate termination of access and/or disciplinary action by CCSNH including, but not limited to restriction to all CCSNH technology resources and/or denial of employment opportunities with CCSNH. As a recognized agent under the Digital Millennium Copyright Act, CCSNH will act in accord with the provisions of this act in the event of notification of alleged copyright infringement by any user.

d. Compliance: All users who access or use CCSNH Information Technology resources must agree to comply with the CCSNH Information Technology Acceptable Use Policy. (also referenced in Student Section 730.08)

Addendum A: Example Violations of Acceptable Use Policy

The purpose of this addendum is to provide examples of violations of CCSNH's Acceptable Use Policy. The following is not an exhaustive list and if you are unsure whether any use or action would constitute a violation of this policy, please contact your campus Information Technology department or the System Office for assistance. In cases not covered explicitly by the CCSNH Acceptable Use policy the System Office determination will prevail.

Examples which Apply for ALL Users (Students, Faculty, Staff and Contract Employees):

Authorized Access/Accounts

1. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account. This includes accessing data not intended for the user, logging into a server or account you are not expressly authorized to access, or probing the security of systems or networks.

2. Supplying or attempting to supply false or misleading information or identification in order to access CCSNH's technology resources.

3. Sharing your passwords or authorization codes with others (computing, e-mail, Blackboard, Banner, etc.).

4. Using technology resources for unauthorized uses.

5. Logging onto another user's account (without the permission of the account owner)

6. Sending e-mail, messages, etc. from another individual's or from an anonymous account.

7. Unauthorized use of CCSNH registered Internet domain name(s).

8. Changing your issued machine name to a name that is different from that assigned by CCSNH or campus Information Technology departments without authorization.

9. Connecting computers or other devices to the CCSNH network that have not been registered with, or approved by, CCSNH.

Services

1. Attempting to interfere with service to any user, host, or network. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service, port scans and attempts to "crash" a host.
2. Use of any kind of program/script/command designed to interfere with a user's computer or network session or collect, use or distribute another user's personal information.

3. Damaging a computer or part of a computer or networking system.

4. Knowingly spreading computer viruses.

5. Modifying the software or hardware configuration of a CCSNH owned computer with malicious intent

6. Excessive use of technology resources for "frivolous" purposes **unrelated to the academic or administrative work of the Colleges,** Examples are game playing

(local or networked), downloading of music/video media files, using peer to peer file sharing programs, listening/watching streaming audio/video feeds (Internet radio, Internet TV, YouTube, etc.). These examples can cause congestion of the campus network and Internet connection or may otherwise interfere with the academic and administrative work of others, especially those wanting to use public access PCs or network and Internet resources.

7. Violating copyright laws.

8. "Hacking" on computing and networking systems.

9. Using technology resources (networks, central computing systems, public access systems, voice and video systems) for new technologies research and development without review and authorization from the CCSNH Information Technology office.

10. Deployment of wireless access points (WAPs) without review and authorization from the CCSNH Information Technology office.

Software, Data & Information

1. Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.

2. Violating software licensing provisions.

3. Installing software on public access and other CCSNH owned computers without appropriate authorization from the CCSNH Information Technology office.

4. Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on CCSNH owned computer equipment or on the CCSNH network.
5. Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Email/Internet Messaging/Voice MailVoice Services

1. Harassment or annoyance of others, whether through language, frequency or size of messages, or number and frequency of telephone calls.

2. Sending e-mail or voice mail to any person who does not wish to receive it, or with whom you have no legitimate reason to communicate.

3. Sending unsolicited bulk mail messages ("chain mail", "junk mail" or "spam"). This includes bulk mailing of commercial advertising, informational announcements, political tracts, or other inappropriate use of system e-mail distribution lists. Forwarding or otherwise propagating chain e-mail and voice mail and pyramid schemes, whether or not the recipients wish to receive such mailings. This includes chain e-mail for charitable or socially responsible causes.

4. Malicious e-mail or voice mail, such as "mailbombing" or flooding a user or site with very large or numerous items of e-mail or voice mail.

5. Forging of e-mail header or voice mail envelope information. Forging e-mail from another's account. Sending malicious, harassing, or otherwise inappropriate voice mail from another's voice lines.

6. Falsely representing opinions or statements on behalf of CCSNH or others.

CCSNH Hosted, and personal Web Pages, Blogs, or other Social Media Web Sites

1. Posting content on personal Web Pages, Blogs, or other Social Networks that provides information on and/or encourages illegal activity, or is harassing and defaming to others.

2. Linking from personal Web Pages, Blogs, or other Social Networks, whose content violates CCSNH policies, local, state, and/or federal laws and regulations.

3. Running personal Web Pages, Blogs, or other Social Networks that support commercial activities or running server systems under the CCSNH registered domain name, CCSNH.EDU or variation thereof, without authorization.

4. The use of the CCSNH name, seals, images and text are the property of CCSNH and shall not be used without the written permission of CCSNH.

Listservs, Bulletin & Discussion Boards

1. Posting a message whose subject or content is considered unrelated to the subject matter of the listserv, bulletin or discussion board to which it is posted. For moderated listservs, the decision as to whether a post is unrelated will be made by the moderator. For listservs that are not moderated and discussion boards, we employ the practice of "self-policing" -- that is, members serve as moderators, commenting (to the sender, to the list) about inappropriate posts.

2. Posting chain letters of any type.

3. Forging header information on posts to listservs, bulletin or discussion boards.

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Information Security and Access Program Policy	Date Approved: September 16, 2010
Policy #: 321.02	Date of Last Amendment: Sept. 16, 2010
Approved: Richard A. Gustafson, Chancellor	Effective Date: October 1, 2010

321.02 INFORMATION SECURITY AND ACCESS PROGRAM POLICY

1. Banner Access

Banner access is restricted to CCSNH employees or third party contractors who have work related responsibilities requiring that access. Unauthorized or illegitimate use of the Banner system or data may result in disciplinary action.

When logging into the Banner system, the Banner account holder understands and agrees to abide by the following:

a. Access to Banner is granted to a CCSNH employee/third party contractor solely to perform appropriate and authorized job functions. Confidentiality of the information/data accessed must be protected. Data should be accessed and/or modified only with a legitimate purpose in completing work assignments.

b. For enhanced security Banner passwords are periodically expired and must be re-created (old passwords cannot be recycled). An individual's password(s) must not be shared with or used by any other person who holds a Banner account. Banner passwords must not be disclosed to any unauthorized individual to gain access to the Banner system.

c. When handling Personally Identifiable Information (PII) in paper or electronic formats:

- Use of PII should always be as restricted as feasible.
- If you are not at your desk, do not leave reports containing PII displayed on your computer screen or unsecured on your desk so others may see their content.
- All paper reports or files containing PII should be secured when not in use and should be shredded or deleted when they are no longer needed.
- PII which resides on portable devices (e.g., laptops, USB drives) should always be encrypted. Upon inquiry, College IT staff will provide information on the CCSNH supported encryption software.

d. Due to the inherent security risk with wireless connections, access to Banner through a wireless connection requires the use of CCSNH issued Virtual Private Network (VPN) software.

e. The CCSNH supplied VPN (Virtual Private Network) software should always be used for remote access to Banner. The VPN software provides a private connection through the public Internet. Upon request, College IT staff will provide a copy of the VPN Request Form. Once the Request is approved the VPN software installation process can be done on any authorized CCSNH computer.

f. The CCSNH issued computer should be the only authorized computer used to access the Banner system. College IT staff have the responsibility to maintain CCSNH issued computers with automatic software updates. These updates provide Operating System modifications and upgrades, to protect each computer against viruses and other dangerous software which might compromise the computer and any information on it. To enhance security, each CCSNH computer should be used for work related purposes only. Personally owned computers are not permitted to access the Banner system or other CCSNH data systems storing Personally Identifiable Information, since these computers are not maintained or secured by CCSNH IT.

2. General Access to Data containing PII:

a. Unless there is a demonstrated need to be mobile with a laptop, a desktop computer is strongly recommended. A laptop computer is a frequent target for theft due to its mobility and should not be the first choice to access Banner or to store PII. If a laptop is required then a lock down cable should be issued and used to secure the laptop.

b. If PII must be stored on a CCSNH issued computer (laptop or desktop) or other storage devices (e.g., external hard drives, USB drives, etc.) this information must be encrypted and password protected using the CCSNH supplied encryption software. Upon request, College IT staff will assist with installation of this software.

c. Personally identifiable information should not be sent using email or FAX facilities unless there are secure processes in place (secure FAX locations, follow up with receiver to be sure the FAX or email has been received, etc.).

d. Copiers and multi-function printers (MFPs) have the ability to store documents/images on internal hard drives which must be permanently deleted by the leasing company or IT before the device is released or discarded. Proof of the deletion is required for College records.

e. When laptops, desktops and other computer equipment capable of storing data are reassigned or discarded, the data must be permanently deleted on the

equipment by the College IT department. Proof of the deletion is required and must be kept with IT records.

f. If data containing PII is maintained outside of Banner, in the form of files on a computer or on a storage device, the data must be secured by enterprise encryption software provided by the CCSNH.

g. If data containing PII is shared with another system, reasonable efforts must be made to ensure the other system, if under CCSNH control, is secure. If the other system or entity is not under CCSNH control, appropriate written releases must be obtained to transmit the data. The releases must convey the authority and responsibility of securing the data to the other entity (either through a contract or Memorandum of Understanding) so that the CCSNH no longer retains responsibility for securing the date.

h. Immediately upon termination of employment or contract, employee or third party contractor access (physical or electronic) to data with PII must be removed.

i. If it is questionable whether a system contains PII, the system must be treated as if it does contain PII (the ISAP applies).

j. Any suspicious behavior or potential data breaches such as lost laptops or storage devices with stored Personally Identifiable Information must be reported immediately to the College Banner Coordinator or to the System Office Banner IT staff (if the Banner Coordinator is not available). Once reported, the *"Data Breach Notification Process"* must be followed (see below).

3. Data Breach Notification Process

The CCSNH is legally required to notify the New Hampshire Attorney General's Office of any data breaches per TITLE XXXI TRADE AND

COMMERCE CHAPTER 359-C, RIGHT TO PRIVACY, *Notice of Security Breach, Section 359-C:20*.

When the Banner Coordinator or System Office Banner IT staff (or any other person) is notified of a suspected data breach of a CCSNH system, notification must be made to the College President, the CCSNH Chancellor's office and CCSNH legal counsel. This group must work to:

a. Identify and document how the breach occurred.

b. Identify the individuals whose Personally Identifiable Information may have been compromised.

c. Identify the potential harm to these individuals by the breach.

d. Determine the impact of the breach and whether external notification is required.

e. Determine ways to assist the individuals affected by the breach.

f. Determine the best notification process to the impacted individuals (the source, content and method).

g. Notify the New Hampshire Attorney General's Office.

h. Follow up: Identify how this process can be improved and how to avoid future data breaches.

4. ISAP Review, Updates and Employee Awareness

State and federal laws change over time and may affect the handling and storage of PII. Any implementation of new services that access PII must be reviewed for compliance requirements. Any new requirements must be identified and followed.

To remain current, the ISAP must be reviewed annually (or sooner if situations dictate). The CCSNH CIO, in consultation with the Chancellor and the System Leadership Team, must perform this review and update the ISAP as required.

This program, policies and any critical training will be disseminated to all CCSNH employees using the CCSNH Intranet (SysNet).

5. Those Impacted By This Program:

All CCSNH faculty, staff, student workers and contract workers are directly affected by this policy.

6. References

a. FERPA of 1974 as amended (Also known as Buckley Amendment)

b. The CCSNH IT Acceptable Use Policy - adopted by the CCSNH July 2009

c. Red Flags Policy on Identity Theft - adopted by the CCSNH May 2009

d. Banner Data Standards And Guidelines

e. New Hampshire Government website

f. The Community College System of New Hampshire website

g. Massachusetts Written Information Security Policies (WISP)

h. "Office of Inadequate Security" - DataBreaches.net

Section: 300 – Human Resources	Subject: 320 Employment
Policy: CCSNH Issued Email Addresses For Faculty and Staff	Date Approved: November 18, 2008
Policy #: 321.03	Date of Last Amendment: Nov. 18, 2008
Approved: Richard A. Gustafson, Chancellor	Effective Date: November 18, 2009

321.03 CCSNH ISSUED EMAIL ADDRESSES FOR FACULTY AND STAFF

It is required that all CCSNH faculty and staff use the respective college/system email address (CCSNH.edu) for all communication with students and other official business of the college/system. Forwarding of CCSNH email to personal email addresses will not be permitted. Forwarding exceptions will be made (e.g. extended illness) only with the permission of the college President or his/her designee.

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Social Media	Date Approved: February 15, 2011
Policy #: 321.04	Date of Last Amendment: Feb. 15, 2011
Approved: Richard A. Gustafson, Chancellor	Effective Date: March 1, 2011

321.04 SOCIAL MEDIA

The following outlines the CCSNH policy on social media, including Facebook and MySpace. Facebook and MySpace are online social utilities that allow individuals or groups of individuals to create a place for a group of people to come together online to post information, news, and events. College pages on MySpace and Facebook are intended to provide the college community with a venue to share thoughts, ideas, and experiences through discussions, postings, photos, and videos. Publication guidelines will be similar to any other media.

It is further understood that each college and the CCSNH System office will have their own internal approval processes to carry out the policies enumerated below.

1. The Communications Director or other individual(s) designated by the President or Chancellor shall approve all sites that can be used for college or CCSNH business. If an employee wishes to submit a site for consideration, a request must be submitted in

writing to the Communications Director or designee. Contributors to college or CCSNH pages will follow the established employee and student guidelines. Oversight of all affiliated pages is the responsibility of the college Communications Director or designee, who will periodically review pages to ensure college policies are followed and that pages are produced in accordance with the best interests of the college.

2. If the college or CCSNH logo is to be used, it must be approved by the college's or CCSNH's Communications Director or designee who must be notified of exact use. No portion of the logo may be altered; colors and fonts must remain as in original file sent from the Communications Director or designee. The logo may not be placed on a background that impairs readability of the mark. Preferred color background is white. Additional art or logos may not be attached to the logo. The college or CCSNH logo should not be used on any personal social media sites.

3. No photos may be placed on a college sponsored page or site without prior approval from the Communications Director or designee. Photos of the college should be provided by the Communications Director or designee whenever possible. The Communications Director or designee reserves the right to remove photos and video images that misrepresent the college or CCSNH or are not of acceptable quality or have been posted without permission or in violation of federal or state law. Whenever possible, a watermark should be added or images should be posted at 72 dpi and approximately 800x600 resolution to protect the college's intellectual property.

4. Because the technology that drives Web communication changes rapidly, this policy may be adjusted to reflect issues that may arise in the management and implementation of the page or for any other reason that supports the college's or CCSNH's priorities for the page.

General Guidelines

1. If an employee has questions about whether it is appropriate to write about certain kinds of material in an approved college or CCSNH site, he/she should consult with a supervisor beforehand.

2. If an employee is authorized by a supervisor to represent the college or the System in social media, he/she should so indicate. If the employee chooses to post about the college or the CCSNH on personal time, the employee should identify himself/herself as a college or CCSNH faculty or staff member, especially when promoting the college or CCSNH through social media.

3. References to college or CCSNH information should always cite the college or CCSNH website as providing the most accurate and updated information.

4. Do not post confidential or proprietary information about the college or CCSNH students, alumni or fellow employees.

5. As stated in the Acceptable Use Policy, college and CCSNH computers and work time are to be used for college/CCSNH-related business. It's appropriate to post at work if comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem. Maintain personal sites during personal time using non-work computers.

Personal Site Guidelines

1. The CCSNH employee is a citizen and a representative of an educational institution or system. When an employee participates in a social networking environment, he/she should be free from institutional censorship or discipline. However, the employee should remember that the public may judge the employee and his/her college or the CCSNH system based on those utterances. Hence, the employee, when participating in a social networking site, should attempt at all times to be accurate, exercise appropriate restraint, show respect for the opinion of others, and not subject the institution or the CCSNH system to public embarrassment or negative attention.

2. The employee is legally liable for what is posted on his/her own site and what they post on the sites of others.

3. The use of the college or CCSNH System logo, or any other college or CCSNH System marks or images on a personal online site is prohibited.

4. The use of the college or CCSNH System name to promote or endorse any product, cause or political party or candidate is prohibited.

5. Since the CCSNH is best served in an environment characterized by professional and ethical behavior on the part of each member of its community, CCSNH respects the individual rights of its employees. However, it also recognizes its responsibility to communicate to the CCSNH community the professional risks associated with participation in a non-work related social networking sites that encourages social interaction between students and faculty and/or staff. If an employee enters into such a social interaction, the employee risks being exposed to complaints that may call into question his/her integrity and professionalism. Therefore, it is the position of the CCSNH to encourage faculty and staff to exercise caution in knowingly becoming "friends" on a social networking site sponsored by a student or when inviting students as "friends" on the faculty or staff person's personal/private social networking site.

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Ethical use of the Data Warehouse	Date Approved: March 15, 2011
Policy #: 321.05	Date of Last Amendment: March 15, 2011
Approved: Richard A. Gustafson, Chancellor	Effective Date: March 15, 2011

321.05 GUIDING PRINCIPLES OF INSTITUTIONAL RESEARCH IN THE ETHICAL USE OF THE DATA WAREHOUSE

The Community College System of New Hampshire (CCSNH) has established one data warehouse repository holding the academic and financial data of all seven colleges in the system. Colleges have been issued licenses for Cognos, a data extraction and reporting tool, to interface with the data warehouse. These licenses permit shared access to reports and data contained across all seven colleges in the system.

The Association for Institutional Research (AIR) in its Code of Ethics suggests that each institution develop a local code of ethics:

> *'IV (b)* ***Development of Local Codes of Ethics.*** *The institutional researcher should develop and promulgate a code of ethics specific to the mission and tasks of the institutional research office and should strive to cooperate with fellow practitioners in the institution in developing an institution-wide code of ethics governing activities in common. The institutional researcher should take reasonable steps to ensure that his/her employers are aware of ethical obligations as set forth in the AIR Code of Ethics and of the implications of those obligations for work practice.'*

As an overarching principle, these data and extraction tools will only be used by CCSNH employees with a legitimate educational interest. In addition to the Information Technology Acceptable Use Policy of the CCSNH (#321.01, effective July 1, 2009) and the Information Security and Access Program (#321.02, effective October 1, 2010), the following guiding principles shall govern the ethical use of the data warehouse and the Cognos data extraction and reporting tools:

- All efforts will seek to create a culture of evidence-based best practices through the establishment of common definitions, language, policies, and procedures related to the design of research projects and the collection and distribution of data.

- In accordance with FERPA, when creating reports for public dissemination, the end user will determine appropriate cell size so as to safeguard the confidentiality of any individually identifiable information.

- Access to other CCSNH colleges' data may be utilized for CCSNH aggregate comparison reporting, such as for establishing benchmarks for program assessment

or when expressly requested by another institution, with the results shared with the institutional researcher of the college with the originating data.

- Any reporting template residing in a public folder may be shared access, with the responsibility for the accuracy and efficacy of the report on the end user, not the report creator.

- In the interest of professionalism and to improve the system for all CCSNH end users, effective and reliable reports, tools, perceived errors or anomalies in data or in data extraction methods and reports will be shared, and source data and methodologies will be documented.

Any violation of these guiding principles will be subject to the provisions of the CCSNH Information Technology Acceptable Use Policy: #321.01.3, Enforcement.

Section: 300 – Human Resources	Subject: 320 Employment
Policy: Shared File Space Guidelines	Approved: July 19, 2011
Policy #: 321.06	Date of Last Amendment: July 19, 2011
Approved: Richard A. Gustafson, Chancellor	Effective Date: July 19, 2011

321.06 SHARED FILE SPACE GUIDELINES

Shared file space is a convenient way for users to securely share files within a department, across departments, within a workgroup or across Colleges. Shared file space eliminates the need to email or otherwise distribute files for others to view or edit.

When shared file space is established, it generally means a directory is created on a fileserver within the CCSNH network where the files to be shared are stored. Authorized users can then access the network fileserver and the shared directory using the secure CCSNH network. This allows users to work with (view or edit) one copy of the same file which can reduce the confusion of multiple edited versions.

Purpose of Guidelines

1. Since shared file space has become a popular method for multiple users to work with electronic documents, guidelines need to be established to set standards for creation, tracking, maintenance and security of shared file space at the CCSNH.

Scope of these Guidelines

1. These guidelines apply to all CCSNH file sharing services hosted on Chancellor's Office central or on distributed College fileservers. In addition, a best practice is to avoid putting files which contain Personally Identifiable Information (PII) in the shared file space. However, if there is a business need to do so, please be aware there are CCSNH policies (Information Security and Access Program) as well as State and Federal laws that will apply to the handling and storage of PII.

2. Sharing of CCSNH files through other methods such as creating shared file space on your computer for others to use or using hosted web sites to share CCSNH files is strongly discouraged as these services are not maintained or secured by Chancellor's Office IT staff or College IT staff. Accordingly, these methods are not part of the scope of these Guidelines.

Shared File Space Guidelines

1. Ownership and Responsibilities

   As noted above, shared file space consists of a network folder that can be used for storing files which are viewed or maintained by multiple authorized users. Generally, the sharing of folders is among users in a department but can be extended across departments or can include individuals within a CCSNH workgroup. The Chancellor's Office IT staff maintains fileservers at the Chancellor's Office and there are also fileservers maintained by College IT staff so for the purpose of these guidelines IT could mean either group. If you have any questions or concerns, the best place to start would be with your local IT staff. The guidelines are:

   - Access and use of shared file space is governed by applicable CCSNH policies which include, but are not limited to the IT Acceptable Use Policy and the Information Security and Access Program
   - Shared file space is to be used for CCSNH administrative or academic work only. Personal files (e.g., personal photos, video, resume's etc..) that are not related to the work of the CCSNH should not be placed in shared file space
   - Shared file space is intended for files you want to share with others, not for storing software applications or a backup of your computer. Note: Exceptions to this guideline can be made for departments such as IT which may keep work related master backups of system configuration files and application installations in shared file space for ease of distribution
   - At least one user must be designated as the "Administrative Contact" for the shared file space. The Administrative Contact has the following responsibilities:
     i. Notify IT who will be authorized to gain access to the shared file space
     ii. Notify IT when a user is no longer authorized to have access to the shared file space Note: Users who have a change of employment

status which affects file share access will not have their access automatically updated. It is the Administrative Contact's responsibility to notify IT in a timely manner of any changes in a user's access

iii. Notify IT how long shared files need to be kept for archival purposes
iv. Maintain folder/file level access for each authorized user. IT can help you establish read (view) only or read/write access for your authorized users. If there are problems or questions with access please contact your IT department
v. Conserving disk space by deleting old or unused files
vi. Notify IT if more disk space is required for the shared file space. Requests for more disk space may prompt an inventory of what files are currently in the shared file space. Since disk space is a limited resource alternatives to additional disk space may be recommended

- IT provides secure back-up for shared file space for the purpose of restoring deleted or lost CCSNH files
- CCSNH shared file space is only available when accessed through the secured CCSNH network or remotely by using CCSNH's VPN software
- Although shared file space provides a secure location to share files with other CCSNH employees it is a best practice to avoid storing files in shared file space which contain Personally Identifiable Information (PII). However, if there is a business need to do so please be aware there are CCSNH policies (Information Security and Access Program) as well as State and Federal laws that will apply to the handling and storage of PII.

2. Establishing Shared File Space

To request shared file space please provide the following information in writing (email is good) to your local IT department (If you have any questions about the information requested please contact your local IT department):

- Provide a statement of need and purpose for shared file space
- Provide the Administrative Contact name and names of others who will be authorized to access the shared file space
- Provide initial access levels to folders and/or files by the authorized users. For example: The Administrative Contact will normally have full view and edit access (read/write access in IT lingo). Then based on the business need of the additional authorized users they could be assigned read (view) only or full access so they can edit files. IT will setup the initial access levels and then the Administrative Contact will maintain or change user access levels as business needs change. If there are questions or problems with access your IT department can help
- Provide an estimate for the initial size of the shared file space – how many files, how large is each file, what is the anticipated growth?
- For legal or compliance purposes how long does an archival copy of the files in the shared file space need to be kept for?

3. User Access

   Requests to add or remove users from the access list of a shared file space will need to be initiated by the Administrative Contact via their local IT department.

   Note: Since there is not a way to automatically update user access across systems if there is a change in employment status which affects a user's file share access it the responsibility of the Administrative Contact's to notify IT in a timely manner of this change in user access.

4. Compliance

   Audits will be managed by the CCSNH Internal Audit Department with the assistance of Chancellor's Office IT staff and/or College IT staff, in accordance with CCSNH Audit Policy.

5. Shared File Space Not Maintained by CCSNH

   Sharing of CCSNH files through other methods such as creating shared file space on your computer for others to use or using hosted services on the Internet to share CCSNH files is strongly discouraged as these services are not maintained or secured by your IT staff.