Carson-Newman Information Technology

Carson-Newman Employee Information Technology Policy

Information Technology Policy
Carson-Newman College
Faculty & Staff

Computer Accounts

Creation of computer accounts
Computer accounts, including a C-N e-mail address are normally created within two business days for new faculty & staff after completing the appropriate paperwork with the HR office.   Early creation of accounts requires approval from the appropriate Executive Council member. Accounts will only be created for employees of the college or others having official business with the college.

Termination of computer accounts
Computer accounts are suspended immediately upon termination of employment and purged after thirty days. Access to the e-mail and/or files from the account can be made available for up to thirty days at the request of the supervisor of the employee.   An extension beyond thirty days requires approval from the appropriate Executive Council member. Retired employees may request to keep their C-N account and/or remain on the faculty or staff e-mail list. Any account that is inactive for more than 180 days is subject to being purged.

Other computer related accounts
Other types of computer accounts (e.g. Datatel) will be created as necessary for the employee and will follow the same policy for creation/termination as the primary computer account.

Computer files
All files stored on college owned computers/servers are considered property of the college.

E-mail
All e-mail stored on college owned computers/servers are considered property of the college.

Data Storage Quota

In an attempt to equitably distribute Carson-Newman's limited storage resources, I.T. will abide by the following data storage quota policy.

Exchange Storage (including E-mail, Calendar, and Contacts):

Each employee is allocated 1,000MB (1GB) of storage for e-mail.

If your Exchange storage use exceeds around 75% of your allocation, the system will send you daily warning messages. At 85% utilization, the system will not allow you to send messages. At 100% usage the system will not deliver new messages sent to you. The sender will receive a "bounce" message.

Messages that you have sent count toward your storage usage unless you delete them from the Sent Items folder. Deleted items count toward your storage unless you empty the Deleted Items folder.

Large attachments are the primary cause of a full mailbox. You are encouraged to save attached files to your personal file storage or portable storage (such as a USB thumb drive) and delete the e-mail message to keep your mail quota clear. Groups of people who collaborate on documents are encouraged to save those documents to shared storage instead of e-mailing attachments back and forth.

Network File Storage (M: drive):

Each employee is allocated 1000MB (1GB) of network storage for work related files.
If your file storage use exceeds 90% of your allocation, the system will send you a warning e-mail message. At 100% usage, you will receive a warning e-mail message and the system will no longer allow you to write to your M: drive. Access will be restored once you delete items from this location. Again, you can save space by saving files you will not be using regularly to devices such as a USB thumb drive. Files saved to locations other than a network drive may not be recoverable in the event of a hard drive failure and are the responsibility of the user.
Audio and video media files (MP3, MPG, AVI, MOV, etc.) use a lot of space and should not be stored on shares unless they form an integral part of the official activity for which the share was created. Large amounts of media files saved on a share will invite scrutiny to determine if they are stored there legitimately.

Departmental Shared Storage:

Departmental shared storage areas are allocated space according to a balance of need and centrality to the College's mission. Shares are created for departments or administrative units as requested. Student organizations may have shares created upon the written request of that organization's advisor. Shares are accessible to either a group of people or the entire College, depending on how each share is configured.
Audio and video media files (MP3, MPG, AVI, MOV, etc.) take up lots of space and should not be stored on departmental shares unless they form an integral part of the official activity for which the share was created. Large amounts of media files saved on a departmental share will invite scrutiny to determine if they are stored there legitimately.
Each department, administrative unit or student organization must have one person designated to ensure quotas for these shares is enforced. By default, this will be the director, advisor, or appropriate vice president.

Procedure for raising your storage quota:

I.T. will make every effort to allocate resources in accordance with the College's mission. To request an increase to your mailbox, network share, or departmental share; send a written (e-mail is acceptable) request to the Director of I.T. with the amount of additional space requested and the reason why this space is required. I.T. retains the right of discretion over increases but will make reasonable efforts to accommodate your need.

Network and Internet Usage

Carson-Newman's network policy and procedures are designed to facilitate the sharing of information while protecting valuable electronic resources.

1. **Internet Access** –Users should ensure that Internet resources are used for scholarly or business purposes only. Incidental personal use is permissible if it meets the following criteria:

   - Does not create a security or legal risk for C-N

   - Does not interfere with employee productivity

   - Does not consume more than a trivial amount of technology resources (e.g. downloading audio/video files and/or streaming/radio via the Internet are large consumers of Internet resources)

   - Does not require the installation of any software or hardware unrelated to scholarly or business use

   - Does not constitute inappropriate behavior for a professional work environment

Hubs, switches, and routers – Personal wireless access points are not allowed. Network hubs or other types of network devices not approved by Information Technology are not allowed.

Wired Academic and Administrative networks – C-N employs a technology known as "port security" on wired administrative and academic networks accessed by college-managed and trusted computers. Port security provides full network access to each trusted network device. Unauthorized network devices connected to the network will be unable to access network resources.

CN-Eagles Wireless network – C-N's wireless network is accessible campus-wide. Wireless network connections are routed through the NAC Appliance system. This system requires authentication of the user and security posture assessment of the attached computer. Each authorized C-N user can have a single NAC Appliance session active at one time.

New wiring requests – To facilitate departmentally requested network wiring additions, I.T. will abide by the following procedure:

- Requesting department will notify C-N I.T. of the need.
- C-N I.T. will determine if there is sufficient network infrastructure available to fulfill the request. If not, I.T. will initiate procurement of necessary equipment.
- C-N I.T. will define the project specifications and either:
  o Request a quote from C-N maintenance, or
  o Provide an estimate for the installation
- The requesting department will generate a C-N purchase order for the project requirements.
- C-N I.T. will coordinate with the requesting department and C-N maintenance until the project's completion.

Mass Communication

E-mail

- The e-mail system will be used to send **daily summaries** of all messages which will be linked to full text on EagleNet should the recipient choose to read further.

- **To Send** a daily summary e-mail either send an e-mail using one of these addresses OR post directly to the individual announcement boards on EagleNet.
  -Student daily summary e-mail address: students@eaglenet.cn.edu
  -Faculty daily summary e-mail address: faculty@eaglenet.cn.edu
  -Staff daily summary e-mail address: staff@eaglenet.cn.edu

- This is an **AUTOMATED** summary. Your e-mail will immediately be posted to EagleNet.
  -A daily summary will arrive in your C-N e-mail inbox each afternoon.
  -Faculty and Staff can submit to student, faculty or staff summaries.

EagleNet Announcements

- **ALL** announcements are to be posted on EagleNet, including EMERGENCY (Urgent) announcements. This may be done via e-mail for general and emergency announcements.
- **No commercial solicitation is allowed on EagleNet or in daily announcements**. For-Sale postings will only be located on EagleNet. The seller must post directly on EagleNet in the appropriate For Sale area.
- **No personal solicitations** for money. Any donation requests should be tied to an event or specific organizational cause.
- If posting an event, no more than two reminders should be posted before the event.

Urgent Communications

- All **immediate** mass e-mails with full text will be reserved for *urgent messages which **cannot and should not wait** until the following daily summary.
- Urgent Communications will also be posted to the appropriate EagleNet announcement board.
  - Immediate mass e-mail will be used to send the urgent and emergency messages by Offices of the EC or those appointed by them.

The office sending the immediate e-mail will also send a copy to EagleNet announcement boards, providing the greatest coverage for emergency communication.

*What is an Urgent Communication?
Urgent need is defined as circumstances under which the appropriate college officer reasonably believes that notification of the college community, or a substantial subset, **communicated over the space of several hours, will reduce the risk of personal harm, property damage, or severe negative impact on C-N operations**.

Emergency Text Messages

The text messaging system (cell phones) would be used for only **emergency** purposes, including disaster alerts and notification of an excessive interruption of the other two modes of communication.

Carson-Newman makes EagleNet Announcements available to facilitate the exchange of timely and useful C-N information. Please refrain from posting announcements with no purpose of sharing useful information to the majority of the designated groups (students, faculty, and staff).

Electronic communication that violates college policies and/or local, state, or federal laws and regulations is prohibited. We reserve the right to delete messages that are deemed abusive, libelous, defamatory, and profane or contain hate speech, violate a third party's right to privacy or are otherwise unacceptable.

Personal Computer Connections

Carson-Newman's **I.T. Policy** requires personal computers connected to the campus network to have both updated anti-virus and operating system updates. This helps protect the campus network and your computer. These requirements are enforced by software called *Clean Access (or NAC appliance)*. If your computer fails to comply with the requirements, you will need to remedy the problem before connecting.

Anti-Virus

http://cnweb.cn.edu/NAC/Clean_Access_AV_Support_Chart.pdf contains the extensive list of approved anti-virus programs that meet the *Clean Access* requirements. Many new computers only come with trial versions of anti-virus or anti-spyware software. If these have expired, they will not meet the requirement.
If you prefer, C-N provides a license of Symantec Anti-Virus for each faculty or staff member. If you have a Windows PC (Windows 2000 or greater) or Macintosh (MAC OS X or greater) you can install Symantec by browsing to EagleNet and selecting the I.T. Department.

Operating System Updates

Prior to being fully connected to C-N's network, your Windows computer will be required to have all critical updates installed. The link - **http://windowsupdate.microsoft.com** - can help you confirm your Microsoft Windows computer is up-to-date. Students with Macintosh computers are not currently assessed for this requirement. However, Macintosh users should regularly update their workstation using "Software Update" as vulnerabilities for this operating system continue to grow.

Connecting to C-N's network

Steps to take to connect to the Carson-Newman network:

1. Make sure your computer meets C-N network requirements.
2. Plug your workstation into a network jack or connect to the wireless network, **CN-Eagles**.
3. Open a browser window and attempt to access the Internet.
4. You will be redirected to a site that requires you to log in with your C-N network credentials. Once authenticated, you will be allowed to download and install the latest *Clean Access* software.

Security

Computer Security

Users are asked to turn their computers off when they leave for the end of the day.   The maintenance window is from 3am until 7am each morning. During this time, it is fine for computers to be used, however, they may run a little slower at times and you may be prompted to save your files and requested / forced to reboot.

Account Security

Each user is assigned their own username and password required to access the campus network. This account is to be kept confidential and not shared with anyone. Usernames and passwords are not to be written down or recorded in any manner where it is not secure (e.g. posted on the monitor, on the desk, under the keyboard, etc.)   Violation of this policy will result in the affected account(s) being suspended. Your password will expire every six months by which time you will need to select a new password. You will receive e-mails beginning 21 days before password expiration and a notice at login time beginning 14 days before password expiration (Mac computers will not receive the login notice). You cannot use a previous password and they must be a minimum of 6 alphanumeric characters in length. I.T. will NEVER ask for your password and you should never give it out to anyone.

Information Security

No information considered confidential is to be saved to the local drive of any Carson-Newman computer, but only to approved network locations such as drive m: and shared network drives where available and appropriate. All computer-related disposals must be handled through I.T. to ensure the secure removal of software / information and to ensure equipment is disposed of safely and properly.