Email Management : Access and Security

Who can view my email without my permission?

Typically email administrators have access to your email account but should only view it when troubleshooting technical problems, or if university policies or contractual obligations are violated. If violations occur, you also can expect your supervisors and their superiors to have access to your email accounts.

At UNC: Work-related email is considered a public record. As such, it is subject to discovery in legal actions against the University and/or in public records requests. Email that mixes work-related and personal topics should be considered a public record and should be managed appropriately. Please see the University policy on email usage for more information.

At Duke: While not a public record, work related email is subject to discovery in legal actions against the University.

What policies exist concerning email privacy?

At **Duke**: The Office of Information Technology has a policy on "Computing and Electronic Communications at Duke University: Security & Privacy," which currently is available at http://www.oit.duke.edu/oit/policy/ITACPolicy.html. The policy says, in part, "the ultimate privacy of messages and files cannot be ensured." Therefore, it is not advisable to use email to communicate confidential or sensitive information.

At **UNC**: Information Technology Services has issued the "Policy on the Privacy of Electronic Information," which currently is available at http://help.unc.edu/?id=1677. According to the policy, the university does not inspect or routinely monitor email usage, nor does it guarantee the privacy or security of email systems. Under certain circumstances, access to email on the UNC computer networks may be given to authorized employees or system administrators.

How should I manage personal email that I receive at work?

At **Duke**: According to the policy on "Computing and Electronic Communications at Duke University: Security & Privacy," the university does not restrict the content of material transmitted across its networks. However, users should be aware that the ultimate privacy of messages cannot be ensured and should limit personal usage of university-sponsored email

systems to a minimum. Personal email that is sent or received at work should be deleted as soon as possible or forwarded to a personal account.

At **UNC**: According to the "Policy on the Privacy of Electronic Communication," university email services may be used for "incidental personal purposes." Users should be aware that there is no guarantee of privacy or security of email systems, and that access to email on computer networks may be given to authorized employees or system administrators. Work-related email is considered a public record but personal email is not; however, personal messages may be included in public records requests if they accidentally are commingled with work-related email, or if email mixes work-related and personal topics.

Whether you work at a public or a private institution, email is discoverable in legal actions. Copies of personal email also may exist on backup systems for weeks after you have deleted them from your email account. Check with your systems administrator for more information about your email backup.

Who "owns" email that I send and receive at work?

While email sent or received at work may be considered "private" in nature, U.S. courts have generally held that employees do not have a right to privacy in electronic messages sent or received at work when the employer sponsors the system. Physical "ownership" of email messages should be considered to reside with the employer, although intellectual property rights, such as copyright, may reside elsewhere. For example, if you receive an email from a colleague with an article attached, although the university would physically own the email it would not own the intellectual property rights to the article. Consult your department supervisors or legal counsel for guidance regarding your particular situation.

See "How should I manage personal email that I receive at work?"

What should faculty know about communicating with students via email?

Several FAQs have established that email is neither secure nor private. While it is common that faculty and students will discuss sensitive issues via email, such as grades, advisory issues, or academic progress, both parties should be aware of protections afforded to them and the risks of such communication

At **Duke**, the University Registrar has enacted policies concerning the release of student-identifiable information, in accordance with the Family Education Rights and Privacy Act (FERPA). Every faculty member should be aware of that policy and whether students have waived their right to privacy. At Duke that policy is available at http://www.registrar.duke.edu/registrar/studentpages/student/ferpa.htm.

UNC has a similar policy, available at http://regweb.oit.unc.edu/resources/index.php. Email

correspondence to and from students, if made or received by faculty members or administrators for their own use and not shown to others, falls outside the definition of "education records," according to this policy. Faculty members should continue to be aware of the security issues surrounding the use of email and the subsequent risk to student's privacy; it is not always the best replacement for an old-fashioned telephone call.

Should I discuss sensitive or confidential issues over email?

Email is not always a secure communications medium, and you should have no expectation of privacy when using it.

You should consult your email system administrators and your supervisor to discuss using email to transmit sensitive or confidential information. They can tell you about safeguards in place to protect that information. Your department may have policies against using email in certain cases, such as transmitting protected health information or discussing personnel matters.

Why do I get so much "spam," and what can I do to avoid it?

Unsolicited or junk email ("spam") clogs nearly everyone's email inbox and can affect email system performance, spread computer viruses, and generally be aggravating.

Email software differs, but most packages contain some sort of filtering capability. In addition, there may exist filtering options at a larger, system-wide level. To learn about your email system's filtering functions, contact your email system administrator.

To avoid spam:

- Do not open messages that could potentially be from spammers.
- Don't purchase anything from spammers.
- Be careful where you post your email address online. It might be a good idea to use a personal email address when posting on forums or bulletin boards.
- Don't reply to spam or ask the sender to remove your address from his mailing list if the spam is coming from a site that you do not recognize. Doing so will simply confirm that your email address exists and you may receive even more spam.
- Block spam with filters. Filters are not perfect and may misidentify a legitimate message as spam. When using a filter you may want to have spam directed to a folder so that you can review it before deleting. See your email administrator for more information.
- When registering with a website or creating an account on a website, always choose "do not sell my email address" if you have a choice.

At **UNC**: If you find yourself receiving a lot of unwanted mail, please send these messages to spam@unc.edu. For more information on spam see:
http://help.unc.edu/?id=1366&within=search-1996938847

At **Duke**: see http://www.oit.duke.edu/docs/getsoftware/email.html for more information.

When I delete an email message, is it really deleted?

Email software differs in their deletion functions. Generally, deleting a message sends it to a "trash" folder or marks it with an "x." You must then instruct the system to "empty the trash" folder or purge messages that have been marked for deletion. Some systems can be set to automatically purge deleted messages when you exit the system. Consult your email system administrator to learn about your deletion/purge functions.

You also should inquire about the frequency of backup procedures. Many email system administrators perform backup after hours at night. If a message resides on the system and has not been purged when backup is performed, it may reside on the backup copy for a number of days or weeks, until that particular copy is recycled or erased/reused.

What happens when my office receives a public records request regarding email?

At UNC: According to the "Policy on the Privacy of Electronic Information," email and other data stored on university computers may constitute a public record like other documents subject to disclosure under the NC Public Records Act (NCGS 132). The university evaluates all requests for information submitted by the public. Consult the Office of University Counsel for guidance if you receive such a request.

At Duke: In isolated cases, some Duke email could be subject to disclosure under the NC Public Records Act. For example: email pertaining to a state-funded project located at Duke could fall into this category. Consult the Office of University Counsel for guidance.