



File Management : Access & Security

Who can access my electronic files without my permission?

Typically information technology administrators have access to your computer 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 files.

At **UNC**: Work-related files are considered a public record. As such, they are subject to discovery in legal actions against the University and/or in public records requests. Files that mix work-related and personal topics should be considered a public record and should be managed appropriately. Please see the University policy on acceptable use for more information.

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

Is there a university policy on using my work computer for creating and/or storing personal documents?

Both UNC and Duke have acceptable use policies for computer usage. In general these state that individuals should keep personal usage of university computing resources to a minimum. Please see the UNC policy at: <http://www.unc.edu/policy/aupol.html>, or the Duke policy at: <http://www.oit.duke.edu/oit/policy/CompNet.html>.

What are the university policies regarding computers and privacy?

At Duke: The Office of Information Technology has a policy on "Computing and Electronic Communications at Duke University: Security & Privacy". The policy says, in part, "the ultimate privacy of messages and files cannot be ensured."

At UNC: Information Technology Services has issued the "Policy on the Privacy of Electronic Information". According to the policy, the university does not guarantee the privacy or security of documents or data stored or transmitted across University networks or on University computers. Under certain circumstances, access to files on UNC computer networks may be given to authorized employees or system administrators.

What should I know about keeping potentially sensitive/ confidential records on my computer's hard drive or network space?

Since the ultimate privacy of your files cannot be ensured, you should be cautious when storing sensitive or confidential files on your computer or network space. Some examples may include student grades or personnel files.

What happens if a Public Records request is made of my office for an electronic record?

At UNC: According to the "Policy on the Privacy of Electronic Information," electronic files 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 files could be subject to disclosure under the NC Public Records Act. For example: files pertaining to a state-funded project located at Duke could fall into this category. Consult the Office of University Counsel for guidance.

Is my computer "backed up"? How often? And how long are those copies kept?

Your department IT administrator can provide you with information regarding the policies for backup for your department. In general, most departments do backups of files on the networked server on a systematic basis.

Often you are responsible for backing up any files that you choose to keep on your local drives. If you use a laptop, you may be especially conscientious about backing up your files due to the increased possibility of loss with a mobile computer.

I'm concerned about viruses and spyware. Where can I learn more about that?

At UNC, for current virus warnings see <http://help.unc.edu>

At Duke refer to the OIT Help website at: <http://www.oit.duke.edu/>