

**IT SERVICES**
[Frequently Asked Questions](#)
[For Students](#)
[For Faculty](#)
[For Staff](#)
[Facilities](#)
**Standards & Policies**
[About ITS](#)
[Strategic Plan](#)
**Acceptable Use Agreement - Faculty, Staff, Students**

Permission is granted to faculty, students, and staff by Davidson College for academic and administrative, non-commercial use of its computing facilities and services according to the terms of this policy. The computing facilities and services include, but are not limited to: microcomputers provided for office use, public computer labs, associated peripherals and files, host computer systems, and Davidson College's networks and network services as well as any other machine or network to which Davidson College provides access or is connected. Faculty, students, and staff granted access to computer systems or services may not use them in any way, which deliberately diminishes or interferes with the use of those systems by others

Ownership of the contents of all disk storage on college-owned systems is retained by Davidson College. The College, and its designated staff, may inspect, when necessary as a function of responsible system management or when there is reasonable cause, all files stored on the ITS computers and systems.

On college computers, permission is granted for the use of licensed software according to the terms of the licensing agreements between Davidson College and the software licensors. Anyone using the software agrees to abide by the terms of those agreements, acknowledging that these software programs are proprietary and therefore are subject to copyright or patent restrictions as defined in the license agreements. Users must agree not to copy, transfer, or remove from college facilities any licensed software, including programs, applications, databases, and code. Davidson College's computer facilities, equipment or software may not be used to violate the terms of any software license agreement or applicable Federal or State laws and regulations pertaining to copyright violations.

Accounts on networks, databases and servers are password protected. Accounts are for the sole use of the individual to whom they are assigned and passwords are strictly confidential. Revealing a password to anyone is a violation of this policy. Anyone with reason to believe that someone else knows his or her password must change it immediately. Persons with accounts are responsible for any and all use of their account. All mail and notices originating from a machine are the responsibility of the owner. The amount of disk space available for directories on network servers is limited. Account owners will maintain only active and frequently used files on these servers.

Unauthorized use of facilities and services includes, but is not limited to the following illustrative examples: illegal or criminal activities, including copying or distribution of copyrighted material without permission; sending fraudulent electronic mail; the unauthorized use, deletion or alteration of accounts or files belonging to other users; use, attempted use, or possession in one's account of programs intended to crash the system, fraudulently imitate system responses, or gain unauthorized access to privileges, accounts, data, software, computers, or networks; harassing or intimidating others; interfering with the reasonable and normal use of the facilities and services by others; sending unsolicited email to large groups or forwarding "chain letters;" copying licensed, proprietary software; or deliberately altering or damaging facilities, hardware, software, system files, or operating system software in any way that would prevent or interfere with the intended use of the computer system by others. In the case of student-owned computers connected to the network, this also includes: connecting devices to the campus network to provide connections from outside of the campus;

modifying the network topology (i.e. extension of wiring, transmission of signals), troubleshooting problems with data jacks; setting up servers, bulletin boards, and networked games; using packet capture devices or software without permission.

The College, and its designated staff, will take action necessary to prevent such misuse and may immediately suspend the computing privileges of anyone suspected of violating Davidson College policies. Upon violation of the terms of this policy, the College retains the right to permanently deny all future computing privileges and services. Anyone violating this policy may also be subject to further disciplinary action by Davidson College authorities and, in the case of students, by the Honor Council, as well as legal action by the proper authorities where violations of state or federal law are involved.

Security of hardware, software, or data, whether personally owned or institutionally owned is the responsibility of those who own or use it. Davidson College is not responsible for any hacker attempts, break-ins, viruses, or other unauthorized activities. Securing sensitive data on local or network drives is a responsibility of employment by the College.

Federal regulations govern the use and distribution of information concerning students. A [statement of policy](#) concerning the release of student information is available from the Registrar's office.

Questions about whether a specific use of Davidson College facilities or services is authorized should be directed to the Executive Director for Information Technology. Ignorance of the policies that govern access and use may not be used as an excuse for actions that violate this agreement.

Revised February 16, 2000

[IT Services](#) | [Newsroom](#) | [RSC at Davidson](#) | [Site Feedback](#)

© 2006 Davidson College | Davidson, NC 28035 | Phone 704-894-2000