

Appropriate Use Policy: Durham Technical Community College Computing Resources

Durham Technical Community College provides a variety of computing resources to faculty, staff, students, and (in limited cases) community residents. The appropriate use of these resources, including personal computers, servers, networks, data sets, printers, Internet and Intranet access, and software are the subject of this policy. Restrictions or limits placed on use of college computing resources are intended to protect the resources as well as the integrity of the networks, and to comply with appropriate policies, laws, and regulations. Individual users of college computing resources must acknowledge consent to abide by this policy in order to use the college's computing resources.

The College's Rights

The college owns or leases the computers and owns the internal computer networks used on campus. The college has rights to the software and information residing on, developed on, or licensed for these computers and networks. The college exercises its rights to and does continuously administer, protect, support, and monitor this collection of computers, software, and networks. The college also exercises its rights to and does continuously establish and uphold rigorous standards for ensuring the security, privacy, bandwidth integrity, and data integrity on its computing systems as it deems appropriate. Furthermore, the college reserves its rights as well as exercises its rights to determine the nature and extent of access to computer resources; deny access to computer systems and networks; limit access to certain sites, materials, and programs; and determine who may connect a device to college computer systems as well as designate the specifications for such a device.

The Individual User's Responsibilities

1. **Use college computing resources for instruction, research, learning, and administrative purposes only.** Durham Tech's computers and networks are for uses consistent with the college's mission. They may not be used for outside business projects or personal activities. This policy also expressly prohibits the use of college computing resources for the intentional accessing, viewing, browsing, downloading, posting, or sending of pornographic or sexually explicit material or images.
2. **Respect licensing and copyright laws.** All software installed on or used on Durham Tech computers must be legally licensed for use on the college premises. Copyrighted software should not be copied from computers on campus or installed on campus computers not legally licensed for their use. Licenses for college-purchased software will be kept on file in the Information Technology Services Department (ITSD). All other software licenses that faculty and staff obtain must be maintained by that user and produced upon request for verification. This includes licenses for all software including but not limited to freeware, shareware, and complimentary software provided to college employees. Students are not allowed to load software on college computers unless they are under the direction of a faculty or staff member.
3. **Maintain secure passwords.** Account passwords must not be shared with anyone, unless directed by faculty for instructional needs. Employees and students should use valid passwords that include at least one non-letter character and should change passwords at least every four months.
4. **Protect college computer facilities.** Users must abide by all federal and state laws governing computer use.¹ Users must not attempt to evade, disable, or "crack" passwords or other security

provisions. Also, users must not knowingly install any virus or destructive computer program onto campus computers.

5. **Use computer resources in an acceptable manner.** Durham Technical Community College computing resources must not be used for any purpose which is not consistent with the mission of the college, which is illegal, dishonest, or potentially damaging to the reputation of the college; or which may subject the college to liability. Unacceptable uses of college computing resources include, but are not limited to, the following:

- Destruction of or damage to equipment, software, or data belonging to Durham Technical Community College or to other individuals or entities;
- Disruption or unauthorized monitoring of electronic communications and electronically stored information;
- Disabling or overloading (or attempting to disable or overload) any system or network;
- Infringement of copyright or trademark laws or rights of others (e.g. downloading or distributing pirated software, video, music, or data);
- Violation of computer system security, including but not limited to the unauthorized use of computer accounts, access codes, or network identification numbers and email addresses assigned to others;
- Unauthorized access to Durham Technical Community College's information systems, Intranet, or networked computers;
- Use of computer communications facilities in ways that unnecessarily impede or disrupt the computing activities of other college users;
- Intentional downloading or propagating the distribution of computer viruses, trojan horses, timebombs, worms, or other forms of destructive rogue programs;
- Posting, sending, storing, or intentionally accessing pornographic, obscene, or sexually explicit material or images;
- Posting personal messages or sending mass electronic messages for such purposes as selling, making solicitations to sell, communicating about partisan political activities, or distributing "junk" email such as chain letters or spam;
- Academic or intellectual dishonesty;
- Violation of software license agreements or copyright laws;
- Recreational use such as peer to peer .mpg file sharing (e.g. music or video downloads);
- Violation of network usage policies and regulations;
- Posting, sending, or intentionally accessing material that is inconsistent or inappropriate to the mission of the college;
- Violation of privacy;
- Harassment;
- Libel or slander;
- Fraud or misrepresentation; and
- Use of Durham Technical Community College's logo without prior approval.

Other Limitations and Warnings

1. **Various limits may be imposed on college computing resources and systems.** Users must abide by any limits set.
2. **Privacy when using computing resources and systems is not guaranteed.** While technical and administrative policies are in place for the protection of computer information, computer data security is never perfect. Please be aware of the following:

- Unauthorized computer users may be able to breach security restrictions and gain access to your files.
 - Misdirected email is not uncommon. Your email messages may be seen by unintended recipients at Durham Tech or elsewhere on the Internet. If email is considered confidential, the information should be communicated by other means.
 - Systems administrators and other college employees may require access to files on any Durham Tech computers to perform audits or resolve technical problems.
 - The college reserves the right to monitor email transmission over its internal computer network. Legal mandates regarding confidentiality will be observed by computer staff when accessing data files.
- 3. Computer users are responsible for backing up their own data files unless told that backup services are provided for their system and their files are being backed up.**

Sanctions

Anyone violating this appropriate use policy is subject to the college's student code of conduct, the employees' due process policy, and criminal complaint or civil action for damages. More specifically, any student, employee, or individual willfully engaging in any activity with intent to interfere with, degrade, monopolize, or compromise the campus network, network security, or any of its components shall be subject to disciplinary action to include suspension, expulsion, termination from employment, and/or prosecution.

Agreement to Comply with the College's Appropriate Use Policy

I hereby certify that I have read and agree to comply with the college's Appropriate Use Policy for computing resources.

Printed Name

Signature

Date

¹It is a violation of federal and/or state criminal statutes for a person to knowingly access, or attempt to access, a computer, computer system, computer network or any part thereof, for the purpose of (i) devising or executing any scheme or artifice to defraud; (ii) services by means of false or fraudulent pretenses, representations or promises; (iii) obtaining unauthorized access; (iv) altering, damaging or destroying either computer hardware, software, or data; (v) directing or causing without proper authorization the denial of computer system services to any authorized user of such computer system services; (vi) transmitting a computer virus with the intent to cause damage; (vii) transmitting without proper authorization a program, information, code or command with reckless disregard of a substantial and unjustifiable risk that the transmission will cause damage; or (viii) trafficking in passwords with the intent to defraud. In many cases such violations are felonies and carry penalties of up to ten years in prison [18 U.S.C. 1030; N.C. Gen. Stat. 14-453 to 14-456].