Information Systems Use Policy

I. Purpose

The purpose of this document is to ensure appropriate protection of Darton College networks, computers, servers and the information transmitted over both local and external networks by providing rules and instructions set forth in policies, standards, guidelines, and procedures.

II. Scope

This document and all supporting documents apply to all Darton College network users, including but not limited to full-time, part-time, temporary and adjunct faculty, staff, students, visitors, contractors, and consultants. This includes those affiliated with third parties who access Darton College computer networks. Any use of Darton College's computer network resources is governed by these documents.

III. Ethics and Acceptable Use

Darton College's Ethics and Acceptable Use policy provides for access to information system resources and communications networks within an environment of openness, trust, and integrity. In addition, Darton College is committed to protecting itself and its faculty, staff, and students from unethical, illegal, or damaging actions by individuals using these systems.

The purpose of this policy is to outline the ethical and acceptable use of information systems at Darton College. These policies and rules are in place to enable faculty, staff and students access to information system resources that are safe from unauthorized or malicious use, which could otherwise expose users to risks including virus attacks, network systems and services failures, and loss of data.

- Users are prohibited from using information system resources for which he or she does not have authorization.
- Users are prohibited from using any information technology resource to engage in conduct that is inconsistent with the stated goals and mission of Darton College.
- Information technology resources are reserved for the use of activities related to the college's missions of teaching, learning, research, and outreach.
- Users are prohibited from using any information technology resource while engaging in any activity determined to be illegal under local, state, federal, or international law or in violation of college policy.
- Users are prohibited from effecting security breaches or engaging in malicious use of network communication. This includes impeding or interfering with other user's legitimate use of information technology systems.
- Users are prohibited from using college facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. This includes using the

college's computing facilities and networks to engage in academic dishonesty prohibited by college policy.

- Users are prohibited from using any information technology resource to actively engage in creating, accessing, displaying, procuring or transmitting material that is determined to be illegal.
- Other than for approved academic instruction, and academic research purposes, users are prohibited from using any information technology resource to actively engage in creating, accessing, displaying, procuring or transmitting material that is determined to be pornographic, obscene, discriminatory, threatening, harassing, or intimidating.
- Users are prohibited from using any information technology resource to actively masquerade as someone else by using their E-mail or internet address or electronic signature.
- Users are prohibited from using any information technology resource for non-college related business purposes or for personal gain.
- Users are prohibited from using any information technology resource to send non-business-related messages to large numbers of E-mail recipients.
- Users are prohibited from sharing their logon ID and password with others. As such, users are prohibited from using others' logon ID and password to gain access to any information technology resource.
- Users are prohibited from engaging in any activity intended to circumvent or compromise any device, system or other form of information technology security.
- Users are prohibited from engaging in any activity intended to establish or create a means that might allow an off campus connection to a college owned or college managed information technology resource.
- Except for public access connections, users connecting to Darton College systems outside of the Darton College internal network must be done via VPN or other such technology provided and configured by the Technology Services Division to verify user identity and provide a secure communication channel.
- The college seeks to preserve individual privacy, however in certain circumstances the college reserves the right to routinely monitor any and all components that make up information technology resources.
- Any and all data created, stored or which traverses the college's equipment and or network, is the property of Darton College.

IV. Electronic Mail

Electronic mail, simply referred to as E-mail, is an essential and valuable tool provided to enhance the core functions of Darton College. E-mail should only be used in the manner and to the extent authorized.

- E-mail usage is a privilege extended to authorized users.
- When E-mailing information deemed sensitive, data encryption must be applied.
- Any E-mail created, stored or which traverses the college's equipment and or network, is the property of Darton College.
- There is no expectation of privacy regarding E-mail usage.
- Mass E-mailing (or broadcast E-mailing) to the entire Darton Faculty/Staff population must be done in an ethical manner.
- It is a violation of the Darton College Ethics Policy to use State resources to send mass E-mail messages to all, or nearly all, of the Darton College E-mail users unless those messages are Darton College business related.

V. Anti-Virus Software

Computer viruses are software programs that are deliberately designed to interfere with computer operations, record, corrupt, and/or delete data, and/or spread themselves to other computers and throughout a network. Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms.

- All college owned computers must have campus approved anti-virus screening software installed, enabled, and updated with current virus pattern recognition files.
- Users who suspect their computer system has been infected with a computer virus, malware, adware, phishing attempt, etc. are responsible for immediately notifying the Technology Services Division helpdesk so that the helpdesk personnel can work to eradicate the virus, and ensure up-to-date virus protection software is properly installed and working correctly.
- If a machine is determined to be vulnerable to an attack, the machine administrator shall reserve the right to remove the machine from the network until the problem is corrected.

VI. Data Backup

Routine, periodic backup procedures are essential to help protect against the loss of data and to facilitate a rapid recovery from an IT failure.

- All computer users are assigned storage space, known as their U: Drive, on an Enterprise Systems server. All users are responsible for storing all important information on their assigned U: Drive.
- Network Support Services is responsible for making routine, periodic backups of qualifying data.
    - All users' U: drives, otherwise known as Users' Folders shall be routinely backed-up by Network Support Services.
    - All sensitive, valuable, or critical information residing on Darton servers shall be routinely backed-up by Network Support Services.

- All data critical to the day-to-day operation within Darton shall be routinely backed-up by Network Support Services.
- All data used to support job related functions or which contain key data critical to the day-to-day operation of that job shall be routinely backed-up by Network Support Services.
- All databases resident on Darton servers shall be routinely backed-up by Network Support Services.
- File and system restoration shall be periodically tested to ensure that backup media and systems are working properly.

VII. Data Stewardship and Sensitive Information

Darton College processes and manages various types of sensitive information which is protected under State and Federal regulations, as well as by College Policy. Information determined to be sensitive information includes, but is not limited to:

- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPPA)
- Information protected by the Family Educational rights and Privacy Act (FERPA)
- Social Security number
- Personal identification number
- Credit card number
- Bank account number
- Computer system names, passwords, IP Addresses, MAC addresses

It is important that this sensitive information be carefully managed and made available only to those persons with appropriately permitted access.

- All users are responsible for data stewardship.
- Users are expected to access college information only to conduct college business.
- Users are expected to respect the confidentiality and privacy of all sensitive information.
- Information shall be stored on centralized, college owned servers when at all possible instead of on desktop computers, laptops or any form of portable media.

VIII. Disposal of Media

Darton College shall discard and dispose of sensitive information in a manner that renders it unrecoverable.

- Paper documents and reports containing sensitive information shall be shredded prior to disposal.
- Magnetic and optical media must be processed by the Technology Services Division, who will properly clean and/or dispose of the media.
- Machines being relocated between offices or sent to surplus must be processed by the Technology Services Division, who will properly clean and/or dispose of the hard drive.

IX. Disciplinary Actions

Violation of this Policy or misuse or destruction of information technology resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is not the role of the Technology Services Division to carry out disciplinary actions as the result of an incident, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the attention of appropriate officials. The following guidelines apply:

- Suspected incidents involving the misuse of information technology resources should be brought to the attention of the Chief Technology Officer.
- If it is determined that a misuse violation has occurred, the incident should be brought to the attention of the Chief Technology Officer.
    - If it is determined that a misuse has occurred by a faculty member, the incident shall be brought to the attention of the Vice President of Academic Affairs for the determination of reprimand to be imposed.
    - If it is determined that a misuse has occurred by a staff member, a visitor, contractor, or consultant, the incident shall be brought to the attention of the Vice President of Business and Financial Services Affairs for the determination of reprimand to be imposed.
    - If it is determined that a misuse has occurred by a student, the incident shall be brought to the attention of the Vice President Student Affairs for the determination of reprimand to be imposed.
    - If it is determined that a misuse has occurred and a criminal violation has taken place, the incident shall be brought to the attention of the Darton College Chief of Police.
- If an investigation involving the misuse of information technology resources has occurred, representatives from the Technology Services Division reserve the right to disclose pertinent information with other departments, as necessary.