

# Disposal of Media Policy

## **POLICY:**

Increasing amounts of electronic data are being transmitted and stored on computer systems and electronic media by virtually every person conducting business for Darton College. Some of that data contains sensitive information, including student records, personnel records, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of, that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within Darton College, including contractors and vendors with access to Darton College systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal. Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as usb drives.

## **Rationale:**

The purpose of this policy is to establish a standard for the proper disposal of electronic media containing sensitive data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

## **Standards & Procedures:**

### **Standards:**

***What is electronic media?*** Electronic Media is defined as any storage that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, video tapes, audio tapes, and removable storage such as usb drives.

***What is the minimum standard for disposal?*** All Darton College electronic media should undergo a complete format before the media, or the system containing the media, is surplus or transferred to another department or state agency. If a complete overwrite of the media is not an option, then the media should be destroyed so that the information it is not recoverable without unreasonable time or cost. This standard is necessary to protect all College information, and to comply with software license agreements.

***What is confidential information?*** Confidential Information is important and sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Some examples of confidential information are system passwords or encryption keys, financial records, proprietary information, human resource or personnel records, student records, and patient records. All media that contains confidential information should be overwritten a minimum of three times with software designed to "zero out" media tracks or destroyed. Other confidential information may be defined by federal or state laws such as [FERPA](#) and [HIPAA](#). Examples of solutions for overwriting media are included below. Note: All Darton Server hard drives are drilled for destruction.

**What are my other options for disposal?** Disposal companies can be utilized to remove any media that you wish to have destroyed; some of these companies are listed below.

**What should I avoid?** Removing the partition information from the media, such as using FDisk, is not sufficient. Reinstalling the operating system, without first completing a full media overwrite is not sufficient. Removing the media and disposing of it in any way that does not render it difficult to recover is not sufficient. Using a magnetic degaussing tool is not reliable for every form of media, e.g. modern hard disks may not be completely erased with most degaussing tools.

Software programs that can be used to overwrite media include:

WipeDrive Pro

File Shredder

Eraser

KillDisk

If you have any questions concerning this standard, or if you would like to suggest a tool that can be added to the list please write to [helpdesk@darton.edu](mailto:helpdesk@darton.edu)

### **Procedures:**

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

**Overwriting Hard Drives for Sanitization:** Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101", followed by "11001010", then "10010111"). Sanitization is not complete until the third overwrite passes and a verification pass are completed. A variety of software packages are available on the open market that properly perform this function.

**Destruction of electronic media:** Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, tape reader, audio or video player.

**Disposal of Hard Drives:** Prior to disposal, operable hard drives must be overwritten in accordance with the procedures above. Equipment designated for surplus or other disposal should have a label affixed stating that the hard drive has been properly sanitized.

**Transfer of hard drives within a department:** Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be sanitized per standards, however; since the drive is remaining within the department, the hard drive may instead be formatted prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the Darton College Policies.

**Sending a hard drive out for repair or for data recovery:** The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with Darton, insuring that the vendor will take proper care of the data. Once data is recovered or the hard drive is repaired, the original hard drive must be returned to the owner so that the owner can dispose of it per this Darton College policy for proper disposal of hard drives.

**Disposal of damaged or inoperable hard drives:** The owner must first attempt to overwrite the hard drive in accordance with the procedures above. If the hard drive can not be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer.

**Disposal of electronic media other than hard drives:**

**Transfer of electronic media other than hard drives within a department:** Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as usb drives, floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

**Disposal of electronic media outside of Darton College:** All electronic media other than computer hard drives must be erased, degaussed, or rendered unusable before leaving Darton.

**Violation of Policy:**

If there is a reasonable basis to believe that the proper procedures as outlined in this policy have not been or are not being followed, a report must be filed with the Chief Information Officer. If improperly sanitized electronic media is found, then the media should be reported to the Office of Information Technology.

**Enforcement:**

Any employee found to have violated this policy may be subject to disciplinary action, including but not limited to, termination under the appropriate College disciplinary policy.