PURPOSE

This guideline outlines the privacy, copyright, and environmental considerations that should be addressed by school boards/authorities when redistributing or disposing of computer systems and electronic storage media. Specifically this guideline recommends process for the removal of personal information from equipment, the appropriate use of software licenses and consideration of the disposal of equipment in an environmentally and socially responsible manner.

All school board/authority computer systems, electronic devices and electronic storage media should be cleaned of sensitive personal or confidential data when no longer needed or before reuse to ensure the continued protection of personal and corporate privacy.

The school board/authority must dispose of all technology hardware and software in accordance with legislation, including but not limited to regulating waste and respecting copyright and licensed software.

School boards/authorities should have a hardware disposal and redistribution procedure in place to promote the secure disposal and redistribution of information technology hardware and electronic storage media. This document includes a number of best practices for developing a procedure.

Definitions

Electromagnetic Degaussing is a method of erasing or destroying data stored in magnetic media, such as hard drives, floppy disks, and magnetic tape using a strong magnetic field.

Electronic Storage Media is defined as any device that is used to store or record electronic information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, handheld electronic devices, and removable storage devices such as floppy disks and zip disks.

Overwriting is one method of sanitation and is used to replace previously stored data on the electronic media with a pattern of meaningless random or non-random information.

The RCMP Technical Security Standard for Information Technology (TSSIT) specifies security standards for information technology including media sanitization requirements. Media may be sanitized by using a software application that overwrites the media a minimum of three times by using a degausser or by physically destroying the media.

Sanitizing is defined as the removal of information from electronic media or equipment such that data recovery using standard techniques or analysis is prevented.

Background

A large volume of electronic data is stored on computer systems and electronic storage media throughout the school board/authority. Much of this data consists of sensitive personal or confidential information, including student records, financial data, and personnel records. The school board/authority is covered by legislation that sets forth responsibilities for protecting this information including the _Education Act,_ the _Municipal Freedom of Information and Protection of Privacy Act_ (MFIPPA), and the _Personal Health Information Protection Act_ (PHIPA). In addition, copyright laws and software license agreements protect vendor rights regarding the use of software. Much of the software used by the school board/authority is licensed under special academic licensing agreements which prohibit the transfer of this software outside the school board/authority.

Unauthorized disclosure of sensitive information may subject the school board/authority to legal liability, negative publicity, and monetary penalties. All sensitive information and licensed software must be properly removed when disposing of computer systems with hard drives, PDAs, removable media, and other electronic devices capable of storing information.

Simply deleting files from the media or formatting a hard drive is not sufficient to completely erase data so that it cannot be recovered. In order to prevent deleted information from being recovered the school board/authority needs to overwrite all previous stored data or to destroy the media by physical force or electromagnetic degaussing.

Scope

This guideline applies to all workstation and storage media hardware purchased, owned, controlled or used by the school board/authority, including equipment purchased by the school board/authority on behalf of individuals or departments within the school board/authority, donated equipment, and equipment in any other way obtained and owned by the school board/authority.

Guidelines

- Equipment that is no longer required may be redistributed within the school board/authority, sold, salvaged for parts, donated to an appropriate charitable organization, or disposed of. Equipment that does not meet the school board's/authority's minimum standard for computer equipment and thus cannot be redistributed within the school board/authority is often of little value to sell or donate and generally should be salvaged for parts or securely disposed of.

- All data (including encrypted data) should by default be considered potentially personal or confidential and should be subject to these procedures.

- Once obtained for school board/authority use, all technology hardware and software should be documented and tracked for inventory control in accordance with school board/authority guidelines. All equipment and software should be tracked centrally from point-of-purchase to disposal.

- The proper disposal and redistribution of school board/authority information technology equipment should be coordinated by a centralized department. A method of disposal inventory should be maintained to ensure, on behalf of the school board/authority, that the liability for technology hardware and software has been relinquished.

- Any equipment which is donated, parted, or disposed of, should have a completed disposal record form with description, serial number, date discarded, method of disposal, and purchase value, if any.

- School board/authority-owned electronic devices and computer systems should be sanitized prior to removal from the school board/authority. This includes removing all school board/authority data and licensed software from the equipment.

- Personal and confidential data should be removed from hardware before it is made available for reuse, even within a department or elsewhere within the school board/authority.

- School board/authority-leased computer systems should be sanitized as part of the end-of-lease processing.

- Erasure tools used in the sanitization process should meet RCMP standards and be approved by the school board/authority. Staff members should take reasonable steps to ensure that these tools are used properly.

- Departments and schools should relinquish all obsolete, broken, or unwanted technology items to a designated department for disposal.

- Removable storage media should not be passed on with equipment but instead should be securely erased, retained by the department, or disposed of by secure means.

- Storage media used to store electronic personal or confidential information should not be released outside of the school board/authority for any reason. This includes vendor or manufacturer service, maintenance, repair, or replacement of the device or the host workstation or server, until such time as it has been cleaned of any personal or confidential data or information unless strict contractual obligations have been imposed. Whenever possible equipment repair should be done on-site.

- Non-rewritable electronic media containing personal or confidential information should be physically destroyed when no longer used or no longer needed.

- Rewritable electronic media containing personal or confidential information should be erased in such a way that the data or information on the device cannot be recovered or the media should be physically destroyed.

- A school board/authority employee, who generates, copies, or records electronic personal or confidential information on local or removable media is responsible to safeguard the confidentiality and ensure the integrity of that electronic personal of confidential information. The employee should ensure that proper procedures are followed for any removable storage devices to be disposed of or reused.

- All equipment should be discarded in an environmentally and socially responsible manner. Any disposal of computer systems and media must comply with all environmental regulations. Some electronic equipment is classified as toxic waste and needs to be disposed of accordingly. Whenever possible, electronic equipment should be recycled by an accredited recycling company.

- The destruction of data and software may be handled by a recycling company if there are strict contractual obligations in existence to ensure the destruction of the data and the protection of personal and confidential information.

- This policy, associated forms, and a list of approved disk sanitation software should be published on the school board's/authority's website.

© 2008

Auditing and Evaluating Hardware Disposal and Redistribution

The school board/authority should ensure that hardware disposal and redistribution procedures are subject to regular audits. These audits should address the school board's/authority's compliance with the operational policies, guidelines and procedures. An external body may be retained in order to perform the audit. The school board/authority should endeavour to immediately address any deficiencies or concerns identified by the audit.

The school board/authority should regularly review and evaluate its hardware disposal and redistribution procedures and related procedures and guidelines to determine if they comply with current legislation and are appropriate given current technology. In the event that significant related legislative changes occur, the policy should be reviewed and updated as needed.

References:

Royal Canadian Mounted Police, *Technical Security Standard for Information Technology* (TSSIT), August 1997.

Royal Canadian Mounted Police, *Hard Drive Secure Information Removal and Destruction Guidelines,* October 2003.

Sources

1. Bristol University - Information Services - *Disposal of computer equipment: University policy*
2. Clark County, Washington - *Information Services Equipment Disposal Policy*
3. Eckerd College - *Computer Equipment Disposal Policy*
4. University of Physician and Surgeons - *Workstation and Storage Media Hardware Disposal and Re-Use*