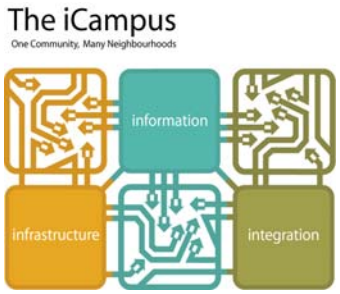
Office of the
Chief Information Officer (CIO)



Enterprise Guideline

MANAGEMENT AND DISPOSAL OF IT ASSETS

April, 2010

Approved


Enterprise Guideline

IT Asset Management and Disposal

Preamble:

This document is one of a series of ***Enterprise IT Guidelines*** published by the Office of the Chief Information Officer (CIO). Guideline documents are distinct from IT Policies (which set institutional requirements) in that Guidelines provide 'best practice' advice to the University community on various topics related to information technology (IT).

The subject of this Guideline is the management and disposal of departmental IT Assets, specifically desktop and portable computing devices. Development of an Enterprise Guideline on this subject was recommended by the University's Audit Services Department. Controls regarding IT equipment disposal, re-use or removal off-site are referenced in Component #5 of the University's newly approved IT Security Policy Framework.

The scope of this Guideline is explicitly targeted to departmental computing equipment (i.e. personal computers, printers/copiers and mobile devices). Other organizational assets such as furniture are outside the scope of this document. Servers and enterprise-level IT assets including major business systems and networking infrastructure are also excluded from this Guideline.

The particular focus of this Guideline includes protecting confidential and/or sensitive information from being inadvertently disclosed; protecting against unauthorized redeployment of University licensed software; and promoting environmental considerations when disposing of obsolete equipment.

It is the responsibility of all Department Chairs/Managers and Unit Heads to maintain adequate records of University owned IT assets. IT assets require distinct tracking and disposal procedures for security and legislative compliance reasons. IT equipment may contain confidential or sensitive information, and may have licensed software installed.

It is especially important that the University takes precautions to ensure compliance with legislation that protects the privacy of personal information. N.B. The University Secretariat maintains a central Directory of Records and Personal Information Banks pursuant to the *Freedom of Information and Protection of Privacy Act (FIPPA).* Department Chairs/Managers and Unit Heads are responsible for securing personal information maintained within their respective units.

This Guideline provides suggestions for:

1) maintaining inventory control of acquired IT equipment and licensed software;
2) ensuring administrative good practice is followed for equipment that is redeployed, recycled, or otherwise disposed of.

Intended Audience:

Primary:	Department Chairs/Managers/Unit Heads, Administrative Assistants, IT Technicians and Analysts
For Information:	All faculty, staff, and students

N.B. This paper provides guidelines to assist University departments. It does not replace or negate existing University Financial, Human Resource, or Research policies and procedures.

Enterprise Guideline

IT Asset Management and Disposal

A. IT Asset Management:

IT Assets encompass 'hardware' (i.e. the physical equipment), software, and information/data. Each of these represents value to the University, but it can be safely stated that data/information is likely to be the most valuable, followed by licensed software, and lastly the physical device.

Unit Heads/Department Chairs are responsible for managing sensitive and/or personally identifiable information which is stored on departmental equipment. The Information and Privacy Commissioner of Ontario publishes guidelines on collecting, using, accessing, disclosing, retaining and disposing of information in compliance with Ontario's *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Personal Health Information Protection Act (PHIPA).*

Each department/unit within the University is expected to maintain a basic record-keeping system for their IT equipment. This Guideline does not propose a specific application solution for maintaining the IT Asset inventory, and in most cases a simple spreadsheet should suffice.

Equipment costing less than $100 (e.g. keyboards) need not be specifically tracked; however any assets which store sensitive data or are directly connected to the University network including printers and copiers with long-term storage regardless of cost should be tracked. The key information that should be maintained for each device includes: date of acquisition, purchased or leased, individual assigned custody, vendor, brand/model, serial number/service 'tag', MAC address, warranty information, licensed (University funded) software installed, date of disposal.

The inventory (or IT Asset Register) should also indicate if the purchased asset will reside off-site (e.g. employee's residence). It is recommended that portable memory devices be tracked by assigned custodian. We recommend that all portable computers be registered with the University "STOP" program.

The University provides a number of secure central services which can be used to store sensitive or personal information. These include Courselink, Gryph Mail, and the Central File Service (CFS) and each has provisions for secure remote access. Department Heads should explicitly authorize all storage of sensitive or personal information on portable devices, and adhere to the University Policy on End-point Encryption.

Departments should develop procedures to ensure assets are returned when employees leave their position.

We recommend that Unit Heads/Department Chairs ensure their departmental Asset Register is maintained as equipment is purchased and redeployed, review their Register annually, and conduct annual physical inventory verification.

Tip! For auditability purposes we recommend that when assets are redeployed or removed, the applicable inventory record is updated/flagged as 'removed' rather than being deleted from the Asset Register.

Enterprise Guideline
IT Asset Management and Disposal

B. IT Asset Redeployment:

There are numerous reasons for equipment redeployment or disposal, and the recommended procedures vary depending upon the action to be taken.

Redeployment which only revises the individual assigned custody is relatively straight-forward unless the equipment is to be relocated off-site.

Suggestions: A review of data stored on the device is strongly recommended.
Determine if there has been any sensitive or confidential information stored.
Remove all sensitive and confidential information as per Section C below.
Itemization of all licensed software on the device is recommended.
Determine if the software licenses are transferable.
Remove any non-transferable software applications prior to re-assignment.
Update the department's inventory record to indicate new individual assigned custody.

Asset disposal requires a more rigorous and documented process. Completion of an IT Asset Disposal Form (Appendix 3) is strongly recommended to document management's decisions, ensure regulations are followed, and the department's inventory record is updated (i.e. the disposal is documented).

Prior to either redeployment or disposal, sensitive information (i.e. confidential or protected) must be removed OR the storage media destroyed! Recommended procedures for both data removal and media destruction are outlined in Section C. of this Guideline.

Disposal may involve **transfer** of equipment to another University department, **private sale**, **sale or gift** to University **employee**, **donation** to an unrelated third-party, or **destruction/re-cycle**. Each of the alternatives listed requires specific steps and are outlined individually below.

1) **Transfer to another Department/Unit:**

Suggestions: Same as above for reassignment within the unit, however completion of an IT Asset Disposal Form is recommended for auditability and the department's inventory record should be updated.
Prior to transfer, sensitive data must be removed! Licensed software may have to be removed.

2) **Donation/Sale to Employee or Third Party:**

Suggestions: Completion of an IT Asset Disposal Form (Appendix 3) is strongly recommended.
A review of data stored on the device is strongly recommended.
Determine if there has been any sensitive or confidential information stored.
If sensitive data has been stored, physically destroy storage media (see Section C).
Itemization of all licensed software on the device is recommended.
Determine if software licenses are transferable.
Remove any non-transferable software applications prior to re-assignment.
Update the department's inventory record


2) **Donation/Sale to Employee or Third Party (Continued):**

Suggestions: (Continued)

Equipment must be assessed as to its Fair Market Value (FMV).
If equipment's FMV equals $500 or more, and is donated to an employee, this is a taxable benefit to the employee and must be reported to Human Resources.
Third-party sales should be openly conducted and documented.
Update the department's inventory record

3) **Recycle or Destroy:**

Suggestions: Completion of an IT Asset Disposal Form (Appendix 3) is strongly recommended.
All data and software must be removed.
If sensitive data has been stored, physically destroy storage media (see Section C).
Utilize the University's Sustainability Office recycling program (equipment is dismantled and recycled in accordance with environmental best practices).


C. Data Removal Guidance:

Guidance regarding data removal is firstly dependent upon whether the equipment/storage media is being redeployed within the University or being disposed of. Data removal by definition is an absolutely irreversible process. Deleting files through 'ordinary' means (e.g. dragging to the trash folder on Windows computers) is NOT equivalent to removal! Recognize however that even sophisticated data removal processes (as outlined below) cannot provide a 100% assurance that data has been destroyed.

If it is known that the equipment stored sensitive University information, and the equipment is being disposed of, we recommend the storage media be physically destroyed and a Certificate of Destruction obtained from a reputable third-party. This action has the advantage of being a high level of due diligence and offers liability protection for the Department Head and the University.

The Information and Privacy Commissioner of Ontario has published a Fact Sheet: Secure Destruction of Personal Information, which includes guidance on contracts with third parties for the secure destruction of records.

The following products and services have been researched by the Office of the CIO and are provided as best practices to ensure information is removed and/or destroyed. Information is current at the time of this writing. Please inform the authors of updates between revisions.

Recommended Products/Tools:

The following tools are recommended for data erasure or disk wiping where it is known that there is no sensitive information involved, and there is a desire to re-use or recycle the equipment. Examples are where there is a requirement to remove licensed software, or non-sensitive data.

Darik's Boot and Nuke
Home page: http://www.dban.org/
DBAN is a self-contained boot disk that securely wipes hard disks of most computers. Consistently rates high in user satisfaction. Free to use in home or business. Offers a bootable image (ISO) download.

Tools Recommended by the RCMP:

The RCMP has published advice regarding IT Media Overwrite and Secure Erase Products. (see reference). At the time of this writing, recommended tools are: Blancco PC Edition by *Inside the box Inc.*; Digital Shredder by *Ensconce Data Technology*; EBAN by *GEEP*; WipeDrive by *WhiteCanyon Software*; and Hammer by *Binatek Inc.*

Additional Tools

Secure erasure tools are often included with other packages which a system administrator may already be using for other applications. These are suitable where there is no sensitive data stored. Examples are:

- G-Disk, which is included as part of Symantec Ghost
- Shred, part of GNU Coreutils
- Mac OS Disk Utility Secure Erase option


Enterprise Guideline
IT Asset Management and Disposal

Recommended Service Providers:

The following Service Providers are recommended for secure data destruction. The brief comments highlight differences in services or commitments at the time of writing. Since these services and associated costs change rapidly in response to market conditions and technological availability, departments are encouraged to confirm service offerings meet their particular needs.

Dell Inc. – Asset Recovery and Recycling Services
Home page: http://www.dell.com/
Service page: http://content.dell.com/us/en/enterprise/services-asset-recovery-services.aspx

Options for onsite and off-site data wipe. Confirmation of Disposal available. Over-writing process is disclaimed as follows: "*No data removal process leaves a hard drive or computer as free from residual data as a new product. Dell makes no recommendations regarding the customer's security needs or representations regarding the effectiveness of one method of data removal over another. It is the customer's responsibility to protect any confidential or sensitive information contained on its hard drives recovered by Dell".*

Recovery Force Inc. – Data Shredding and Drive Wiping
Home page: http://www.recoveryforce.com/
Service page: http://www.recoveryforce.com/media-wipe

Located in Guelph. Options for on-site pick-up. Offers Certificate of Destruction on request. Forensic and local court experience.

Softchoice Inc. – S.A.F.E. Hardware Removal Service
Home page: http://www.softchoice.com/
Service Page: http://www.softchoice.com/about/sustain-enable/ecotech/ewaste/

Hardware removal service. Certificate of Destruction offered. Partnerships with charities and a no landfill, no export recycler. Offers on-site kiosk station for small hardware.

Vanguard Professional Services Inc. – Data Destruction and Recycling
Home page: http://www.vanguardinternational.com/

Located in Mississauga. History in Magnetic Tapes. Offers Certificate of Data Destruction. Advertises $5-million comprehensive liability insurance coverage.

Tip! To minimize costs and encourage participation a department may store a number of devices in a secure area and batch an order for data destruction services.

Enterprise Guideline

IT Asset Management and Disposal

Version/Update History

Second Draft Published:	April 15, 2010
First Draft Published:	March 3, 2010
Initial Authors:	Doug Badger, Gerrit Bos Office of the CIO

Enterprise Guideline

IT Asset Management and Disposal

Appendix #1

Definitions:

Personal Information: A defined term in the *Freedom of Information and Protection of Privacy Act (FIPPA).*

Sensitive Information: Information or data which management considers confidential OR is personally identifiable. Any information which if inadvertently disclosed would be detrimental to the University or in violation of FIPPA or PIPEDA.

Fair Market Value (FMV): The price that would be agreed on between a willing buyer and a willing seller, neither being under any compulsion to buy or sell and both having reasonable knowledge of the relevant facts.

Media Access Control Address (MAC Address): A unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address.

Enterprise Guideline

IT Asset Management and Disposal

Appendix #2

References:

Secure Destruction of Personal Information.
Source: Information and Privacy Commissioner/Ontario Fact Sheet No. 10, December, 2005.

IT Media Overwrite and Secure Erase Products.
Source: RCMP Technical Security Branch IT Security Bulletin B2-002, May 2009.

University of Guelph Human Resources Policy #710:
Service Recognition and other Performance Based Awards

University of Guelph IT Policy:
End-point Encryption

University of Guelph Secretariat:
Directory of Records and Personal Information Banks

Enterprise Guideline

IT Asset Management and Disposal

Appendix #3

SURPLUS IT EQUIPMENT DISPOSAL FORM

Department Name	Building/Location	Chair/Manager	Custodian	Date

Asset ID/Tag#	Serial No.	Asset Type	Disposal Method	Sensitive Data (Y/N)

Description of Equipment (include date acquired and model): _____

_____

_____

If Sensitive Data is marked "Y" above, all storage devices within the equipment must be absolutely erased. The undersigned Manager certifies that this has been accomplished prior to disposal.
N.B. If the equipment is being disposed and not redeployed, it is recommended that storage devices be physically destroyed. A written third-party certification of data destruction is recommended in addition to the Department Head's signature.

_____ _____
Signature of Department Head/Manager Date

_____
Name (please print)

Method of data erasure: _____
_____

If equipment is to be donated or sold, indicate the Fair Market Value: $_____

Donated or sold to: _____
Indicate if employee or third-party (attach receipt)

Disposal Approval: _____ _____
Signature Date

_____ _____
Name (please print) Position