

POLICY TITLE: IT Asset and Data Disposal Policy

Initial Draft By - Position / Date: Information Security – 06/28/2022

APPROVED BY / DATE: Dave Whittle, CIO – January 17, 2023

Last Revised Date: January 17, 2023

Next Review Date: One year after Approval

BRIEF DESCRIPTION: This document describes the processes to properly dispose of IT assets and data to protect University data from inadvertent disclosure.

Table of Contents

Introduction	1
Scope	2
Policy Statements	2
Related Policies, Guidelines, and Processes	4
Responsibilities	5
Implementation.....	7
Exceptions.....	7
Definitions	8
APPENDIX A – Drive Erasing.....	9
APPENDIX B – Securely Deleting Files.....	10

Introduction

This policy is focused on the protection of confidential and sensitive University information from inadvertent disclosure, preventing unauthorized redeployment of licensed software, and promoting environmental considerations when disposing of Information Technology (IT) equipment.

Within this policy, the term IT Asset refers to physical hardware, storage, software, and data. Each of these elements represents value to the University, with data being the most valuable and with the most potential risk, followed by licensed software, and lastly physical devices. IT assets, such as computers, mobile devices, and storage media, may contain confidential or sensitive information and may have licensed software installed. Departments must track these assets and take precautions to protect the privacy of sensitive information when assets are transferred or disposed of, and to ensure compliance with relevant University policies and government legislation.

In the event that [Confidential \(S3\)](#) or [Restricted \(S4\)](#) data is compromised, lost, or stolen it must be immediately reported to the Information Security team and the University Privacy Officer. Depending on the circumstances and the data involved, the University may be required to publicly disclose the incident to the [Information and Privacy Commissioner of Ontario](#) and [Ministry of Colleges and Universities](#).

For information on record retention and disposition, refer to the [University Record Retention and Disposition Policy](#).

Scope

All University-owned IT assets and computing equipment are in-scope of this policy. This includes, but is not limited to, endpoint and portable computing devices, servers, network devices, printers, copiers, mobile devices, and storage media.

Other devices and services hosted on-premises or remotely used to store [Internal \(S2\)](#), [Confidential \(S3\)](#), or [Restricted \(S4\)](#) University information, regardless of device ownership or service provider, are also in scope. This includes computing devices owned by researchers, students, or contractors working on behalf of the University, and those purchased through University professional development programs.

This scope is consistent with legislative requirements, such as [Personal Health Information Protection Act \(PHIPA\)](#) and [Freedom of Information and Protection of Privacy Act \(FIPPA\)](#), and the University's obligation to protect against accidental disclosure of [Confidential \(S3\)](#) or [Restricted \(S4\)](#) data.

Policy Statements

1. All University departments must maintain a record-keeping system for their IT assets both hardware and software. This policy does not mandate a specific solution for maintaining the inventory, however it may be as simple as a manually maintained spreadsheet. This asset inventory must be updated when assets are added, transferred, or disposed of. Contact the [Information Governance and Compliance team](#) for assistance if needed.
2. All University departments must develop procedures to ensure access to sensitive information is reviewed when employees change roles or leave the University. Those procedures must include steps to have all IT assets in the custody of departing employees returned to the University.
3. When IT assets are transferred within the University or disposed of at the end of their useful lifecycle, departments must maintain records to document the reason for retirement and the disposition of the asset. When assets are transferred, departmental record keeping should include the name of the individuals to whom the assets were transferred. Depending on the data involved, a certificate of data destruction may also be required for auditing or regulatory compliance purposes. These records must be maintained for a minimum of 2 years, unless otherwise mandated by University policy or legislation.
4. Prior to redeployment of any IT asset within the University, [Internal \(S2\)](#), [Confidential \(S3\)](#), or [Restricted \(S4\)](#) information must be securely removed. This may be done either by securely erasing data on the physical storage media or destroying the storage media. Recommended procedures for data removal and physical media destruction are outlined in this document's appendices. Assistance can be obtained by contacting the [CCS Help Centre](#).

5. Prior to the transfer or redeployment of any IT asset within the University the asset must be reviewed to ensure:
 - The hardware is capable of running a current, licensed, and supported operating system. All devices connected to the campus network are [required to run a vendor-supported operating system](#) for which security patches are available. Legacy assets that do not meet this requirement must be recycled using the [University E-Waste program](#).
 - Any [Internal \(S2\)](#), [Confidential \(S3\)](#), or [Restricted \(S4\)](#) information is removed, either by secure deletion or physical destruction of storage media. If sensitive data has been removed, retain a certificate of destruction for future reference.
 - All licensed software on the device is either transferred (if possible) or removed. Refer to [University of Guelph Software Licensing Policy and Guidelines](#).
6. If an IT asset cannot be redeployed, the hardware must be disposed of in accordance with environmental best practices, such as through the [University E-Waste program](#) available on the main campus. IT assets must not be sold, donated, or given to persons or organizations outside of the University or provided to employees for personal use due to concerns of legal liability, ongoing support, and equity. **For example**, if a University laptop is donated to an outside party and the battery explodes causing a fire, this could potentially lead to litigation against the University.
7. Prior to computing assets being disposed of using the [University E-Waste program](#), all physical storage (including but not limited to hard drives and solid-state drives) must be removed and physically destroyed by crushing or shredding. CCS offers hard drive destruction as a service through an agreement with a third-party vendor. As part of this paid service, a certificate of destruction will be provided for all destroyed media.
8. When no longer required, removable storage media (including but not limited to CDs, DVDs, USB flash drives, floppy disks, and magnetic tape) storing University data must be physically destroyed by shredding, scratching, cutting, breaking, or other means to render them unusable. Removable storage media may also be sent to CCS for secure destruction.
9. In all cases where University-owned computers, laptops, mobile devices, cell phones, tablets, network devices, or office equipment (including but not limited to routers, printers and copiers) will be recycled, returned, redeployed, or sent off-site for maintenance, a full reset to manufacturer default settings must be performed prior to leaving University custody. This will ensure no University configuration information or data is inadvertently released along with the device. If the device offers the ability to purge data or the capability to perform a cryptographic erase to ensure that data is unrecoverable, that must be completed. If the device contains additional removable storage, it must also be erased or destroyed.

10. University data custodians and data stewards have an obligation to ensure that all data stored in third party hosted services is securely destroyed at the end of a service contract.
11. As part of the selection process for services hosted by a third party, a [Security Risk Assessment](#) must be performed as part of the procurement process to ensure the security of University data and systems. As part of that process, vendors must clearly describe where the University data will be stored, how they will protect data in transit and at rest, and their data destruction process when the contract ends.
12. All exceptions to this policy must be approved by the Chief Information Officer (CIO).
13. In the event that [Confidential \(S3\)](#) or [Restricted \(S4\)](#) data is compromised, lost, or stolen it must be immediately reported to the Information Security team.

Related Policies, Guidelines, and Processes

- [Encryption Policy](#)
- [Data Storage Guidelines](#)
- [Security Risk Assessment Process](#)
- [Record Retention and Disposition Policy](#)
- [Software License Policy](#)

Responsibilities

1) Data Custodians and Data Stewards

- i) University data custodians and data stewards have an obligation to ensure that all data stored in third party hosted services is securely destroyed at the end of a service contract.

2) End Users

- i) End users of personally-owned devices that are used to store [Internal \(S2\)](#), [Confidential \(S3\)](#), or [Restricted \(S4\)](#) University information are also in scope of this policy. As such, they are responsible to ensure that they adhere to the requirements of this policy, related policies and guidelines, and departmental procedures when IT assets are decommissioned or transferred, including ensuring data is properly removed before devices leave their custody.
- ii) In the event of a lost or stolen personal device in-scope of this policy, report it immediately to [Information Security](#).

3) IT Administrators

- i) Understand and adhere to the requirements of this policy, related policies and guidelines, and departmental procedures when IT assets are decommissioned or transferred, including ensuring data is properly removed before devices leave their custody and updating the IT asset inventory.
- ii) In the event of a lost or stolen device in-scope of this policy, report it immediately to [Information Security](#).

4) Managers, Department Chairs, Unit Heads, and Directors

- i) Managers, Department Chairs and Unit Heads are accountable for managing sensitive and personally identifiable information which is stored on departmental equipment in their respective units. They are also responsible for adhering to the University's [Record Retention and Disposition Policy](#). The [Information and Privacy Commissioner of Ontario](#) also publishes guidelines on collecting, using, accessing, disclosing, retaining and disposing of information in compliance with [Personal Health Information Protection Act \(PHIPA\)](#) and [Freedom of Information and Protection of Privacy Act \(FIPPA\)](#).
- ii) Develop and follow procedures for when employees change roles or leave the University.
- iii) Ensure that a record-keeping system for departmental IT assets is in place and maintained.
- iv) Identify IT assets for which they are responsible and ensure asset records are kept current.
- v) Ensure that IT administrators in their unit adhere to this policy when assets are decommissioned or transferred.

- vi) Ensure that a security risk assessment is completed as part of the selection and procurement process for all third party hosted applications and services hosting University data.
- vii) When third party hosted service subscriptions are terminated, ensure that all University data is destroyed.
- viii) Department Heads must explicitly authorize all storage of sensitive or personally identifiable information on portable devices or third party hosted services, and adhere to the University Encryption Policy and Data Storage Guidelines. Where possible, centrally-managed services should be used to securely store sensitive information, such as Microsoft 365 and the Central File Service (CFS).

5) Information Security

- i) Undertake periodic reviews of this policy and associated processes in collaboration with supporting IT groups.
- ii) Provide effective methods and resources to users, IT administrators, and departments to ensure that this policy can be effectively and efficiently implemented.
- iii) Investigate all incidents related to lost or stolen IT assets in coordination with the appropriate IT support teams, Campus Safety Office, the Privacy Officer, and outside agencies as required.
- iv) Follow the CSIRT process as documented in the [Cyber Security Incident Response Process](#) in the event of a major security incident or data breach.

6) Chief Information Security Officer (or designate)

- i) In accordance with the [Cyber Security Incident Management Policy](#), report major incidents to the Chief Information Officer (CIO) and advise the Privacy Officer if a data breach involving University records or personal information is alleged.

7) Chief Information Officer (or designate)

- i) Review and approve exception requests to this policy.
- ii) Review and approve changes to this policy.

8) Privacy Officer

- i) Receive and respond to incidents involving theft, leakage, or compromise of [Confidential \(S3\)](#) or [Restricted \(S4\)](#) University information.
- ii) Coordinate the investigation into [privacy breaches and reporting](#).

9) Chief Internal Auditor

- i) Review compliance on campus through periodic audits of departments administering [Confidential \(S3\)](#) or [Restricted \(S4\)](#) information.

Implementation

From the effective date of this policy, all departments on campus must comply with all aspects of this policy.

Information Security recognizes that the process of implementing some measures will take time and effort by IT staff, however measures to achieve compliance must be undertaken as expeditiously as possible.

Exceptions

Any exceptions to this policy must be reviewed and approved by the CIO. The following information is required to evaluate all exception requests:

1. Requesting campus unit
2. Requesting campus unit director/manager contact information
3. Technical representative contact information
4. Date of request
5. Reason for exception request
6. Description of proposed solution
7. Mitigating security controls to secure sensitive information

Definitions

Data Custodian – Persons who own technical accountability for a set of data assets and maintain that data in accordance with the requirements and policies defined by data stewards. Data custodians protect rights for access, processing, maintenance, storage, protection, and destruction.

Data Stewards – Individuals who own business accountability for a set of data assets, which includes Lead Data Stewards chosen by functional/subject area (e.g., research, student, finance, etc.). Data Stewards are the point of contact for questions about the data definitions, use of the data, and are knowledgeable about existing processes and carriers of institutional knowledge about data in their custody. They also document and guide policies, procedures, and guidelines related to the data in their custody throughout the data life cycle.

E-Waste – E-waste is any electronic equipment that has been discarded. This may include items that are broken, working, or have reached the end of their useful life. E-waste is particularly dangerous due to potentially toxic materials as they decay when discarded or put into a landfill.

IT Asset – Within this policy, the term IT Asset refers to physical hardware, storage, software, and data. Each of these elements represents value to the University, with data being the most valuable and with the most potential risk, followed by licensed software, and lastly physical devices.

Portable Device – Any portable device that can store data such as a laptop computer, unsecured server/desktop, tablet, smartphone, portable storage device (USB drive), or physical media such as CD/DVD, etc.

Personally Identifiable Information (PII) – Personally identifiable information includes information about one's age, race, sex, marital status, educational and medical history, and unique numbers such as SIN or student numbers. PII data may also include non-sensitive/indirect data elements that may not be considered sensitive alone but when combined with other publicly available information, could be used to identify an individual. Refer to the [Freedom of Information and Protection of Privacy Act \(FIPPA\)](#) for additional information.





Internal Data (S2) – Internal data is non-public University information including but not limited to internal documents, contacts, purchase orders, operating procedures, and admission metrics.

Confidential Data (S3) – Confidential electronic information includes but is not limited to personally identifiable information and is defined in the [Data Storage Guidelines](#). In addition, federal and provincial legislation specifies data elements which require protection from unauthorized creation, reading, modification and/or deletion.

Restricted Data (S4) – As defined by the [Data Storage Guidelines](#), restricted data includes data with a high likelihood of harm if compromised, and includes personal health information, financial or banking information, and Social Insurance Numbers.

APPENDIX A – Drive Erasing

In cases where computing assets will be redeployed in accordance with the policy statements above, the operating system and all data stored on that device must be securely erased. To ensure data is unrecoverable, physical hard drives must be erased using one of the following methods. Where technologically possible, the National Computer Security Center (NCSC-TG-025) standard should be used which uses a 3-pass system including verification after each pass of 0s, 1s and a random character.

Product	Cost	Availability	Certificate of Destruction	Additional Information
CCS Drive Destruction Service	\$8 per asset	All platforms		<p>If a certificate of destruction is necessary, the physical storage device should be destroyed by CCS' third-party service which is available for a small fee of \$8 per device.</p> <p>(Cost updated February 2024)</p> <p>Contact CCS for additional information: IThelp@uoguelph.ca</p>
DBAN Hard Drive Eraser and Data Clearing Utility	Free for personal use	All platforms		<p>DBAN is a self-contained boot disk that can securely remove data from most hard disks.</p> <p>Please note that this is only free for personal use. Use for University owned assets requires a valid software license.</p>
macOS Disk Utility Secure Erase	Free	macOS		<p>The built-in macOS Disk Utility has the ability to clean a hard drive by writing over all data multiple times making the original data unrecoverable.</p>
Shred	Shareware	Linux		<p>Part of the GNU Core Utilities, shred is a command for Linux system that securely deletes files or devices so that it is extremely difficult to recover them.</p>

APPENDIX B – Securely Deleting Files

In cases where erasing or destroying an entire hard drive is not warranted, there are options available to securely delete individual files and folders. Simply deleting files in Windows or MacOS operating system does not guarantee that the information is permanently removed. This method of deleting files does not actually erase the data, instead it just marks the space where the files were stored as being available for re-use. Files deleted in this way can be recovered by anyone using easily available data recovery software. To ensure data is unrecoverable, secure deletion tools should be used.

Note that some secure deletion tools do not work on flash-based hard drives like SSD drives and SD cards. For users needing to erase files on flash based hard drives, full disk encryption with Bitlocker (Windows) or FileVault (macOS) mitigates the risk of data exposure since deleted files remain encrypted.

Secure deletion software options include:

Product	Cost	Availability	Additional Information
BC Wipe	Commercial	Windows, macOS, Linux	Ability to permanently wipe files selectively so that they can never be recovered or undeleted.
sDelete	Free	Windows	A command line utility that allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk.
Shred	Free/Open-Source	Linux	Part of the GNU Core Utilities, shred is a command for Linux system that securely deletes files or devices so that it is extremely difficult to recover them.