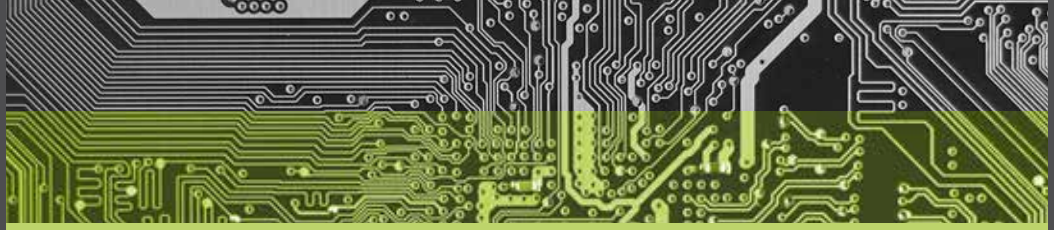

FEBRUARY 2018

TECHNOLOGY
FACT SHEET

Disposing of Your Electronic Media

This fact sheet provides guidance on how Ontario public institutions and health information custodians can securely destroy personal information when disposing of electronic media.

LEGAL OBLIGATIONS

Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*), its municipal counterpart, *MFIPPA,* and the *Personal Health Information Protection Act* (*PHIPA*) require institutions and health information custodians ("custodians") to take reasonable steps to safeguard personal information, including personal health information, from the moment of collection to the point of destruction.

Whether the steps taken are reasonable depends on the circumstances. In every case, you must destroy information in such a way that it cannot be reconstructed or retrieved.

This guidance applies when electronic storage media containing personal information will be disposed of, recycled, reused or otherwise made available to persons outside of your organization. It covers the following media types:

- magnetic media (such as hard drives, magnetic tapes)
- electronic drives (such as solid-state drives, USB flash drives, memory cards)
- mobile devices (such as smartphones, tablets)
- optical discs (such as CDs, DVDs, Blu-ray discs)

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

IMPORTANCE OF SECURE DESTRUCTION

Failing to safeguard personal information exposes your organization to legal, financial, reputational, and other risks. Unauthorized access to, or inappropriate disclosure of, personal information stored on electronic media is a privacy breach and can have significant consequences for the individuals involved.

CHALLENGES TO ENSURING SECURE DESTRUCTION

There are a number of challenges to ensuring secure destruction of digital information, including:

- deleting files or formatting a drive are not sufficient to ensure secure destruction
- the destruction method used must be appropriate for the media
- it may be necessary to purchase special software or equipment
- some software will not work if the media is damaged

This fact sheet provides an overview of the ways in which information stored on electronic media can be securely destroyed. It does not provide detailed "how-to" guidance. As institutions and custodians, you should consult with your information technology advisors to ensure an effective, secure destruction process that complies with Ontario privacy laws.

METHODS OF SECURE DESTRUCTION

To securely destroy personal information, you must perform operations on the *media* where the digital information is stored. There are two ways to securely destroy digital information:

- physically destroy the storage media
- overwrite the information stored on the media

The best method to securely destroy personal information will vary depending on the type of media. Note that some devices, such as printers, fax machines, and smart phones, may contain multiple types of storage media, with each type requiring a different information destruction method.

Physical Destruction of storage media is the most extreme method of ensuring that information cannot be recovered. Specialized tools and services can disintegrate, incinerate or pulverize devices, drives and discs. Magnetic media can also be *degaussed*, which involves applying a strong magnetic field to eliminate the stored information. Degaussing, like other methods of physical destruction, renders magnetic media unusable but it securely destroys all stored information.

Overwriting (sometimes called “wiping” or “sanitizing”) records new and non-sensitive data over the information to be destroyed. Overwriting is carried out by special software, and can be implemented in different ways, depending on the media. For example, some mobile devices come with specialized overwriting software pre-installed that can be used to securely destroy information on the device. In contrast, external software is usually required to overwrite information stored on most magnetic media. It is important to match the overwriting method and tool to the specific media.

Overwriting cannot be carried out if devices are damaged or non-rewritable (such as optical discs), and may not completely address all areas of a device where information is stored. It can be challenging to effectively overwrite electronic drives (as compared to magnetic drives) because they have very different memory systems and therefore overwriting is generally not recommended for electronic drives.

Cryptographic erasure is a special form of overwriting that replaces stored information with strongly encrypted data, often referred to as deletion-by-encryption. Once information is encrypted and the cryptographic keys are securely erased, the personal information is rendered irretrievable. One drawback of this method is that the secure deletion may be difficult to verify by inspecting the media because there is no way to confirm that the cryptographic keys were, in fact, erased.

File Deletion is *not* an acceptable way to securely destroy stored information. Basic deletion operations do not securely destroy information because when a file is deleted from a personal computer, for example, only the pointer or link to the location on the drive where the information is stored is removed. The actual information remains and is not destroyed.

Media Formatting is also *not* an acceptable way to securely destroy stored information. Similar to deleting a file, formatting a hard drive or USB drive only removes the pointers to the location where the information is stored. The actual information remains and is not destroyed.

The chart below provides an overview of secure destruction methods for different devices and media.

Media Type	Recommendation	Considerations
Magnetic media (internal and external hard drives, magnetic tapes)	Overwrite three times **or** Use a degausser to erase the magnetic properties of the stored information. This will render the media permanently unusable. **or** Physically destroy	You may need special tools to overwrite hidden or reserved storage areas It may be acceptable to overwrite one time only if you plan to destroy the media Magnetic media can be disintegrated, incinerated or pulverized
Electronic drives (solid-state and USB "flash" drives, memory cards)	Physically destroy	Overwriting techniques cannot be used to securely destroy information on electronic drives or memory cards Electronic drives should be destroyed by disintegrating, incinerating or pulverizing
Mobile devices (smartphones, tablets)	Physically remove or destroy any removable electronic storage media **and** Overwrite other stored information by performing a full factory reset to default settings in accordance with the device maker's instructions	After completing the full factory reset, you should manually navigate to multiple areas of the device to verify that all information has been destroyed
Optical discs (CDs, DVDs, Blu-ray discs)	Physically destroy	Remove information-bearing layers with a surface grinder or destroy by incinerating, shredding or pulverizing

DATA DESTRUCTION PROGRAM

Destruction is an important part of the information life-cycle and does not take place in isolation from other information management activities. Certain conditions are necessary for an effective data destruction program.

Your organization must have information retention and disposal policies and procedures. You must also appoint a person responsible for keeping these policies and procedures up to date, and providing training to all staff.

Your organization should be able to identify the classification, sensitivity, and location of information holdings, including copies and backups. You should also be able to identify and locate all media containing digital information.

VERIFICATION AND DOCUMENTATION

The secure destruction of digital information should be verified. This may include organizational procedures to document the destruction processes, the effectiveness of the equipment or software used, and the end results.

FIPPA institutions must maintain a disposal record setting out what personal information has been destroyed and the date of destruction.[1] Municipal institutions and custodians are encouraged to keep similar records.

OUTSIDE PARTIES

Institutions and custodians may engage outside parties to securely destroy digital information and storage media. We recommend looking for a reputable service provider and ensuring that the contract, at a minimum:

- spells out the terms of the relationship
- sets out clear responsibilities to securely destroy information
- specifies how destruction will be accomplished
- requires a certificate of destruction upon completion
- allows for inspection of the destruction process
- ensures appropriate training for employees involved
- limits subcontracting
- specifies a time period within which records will be destroyed
- requires secure storage pending destruction

1 R.R.O. 1990, Reg. 459, s. 6 (1).

ADDITIONAL GUIDANCE

For additional information and guidance on the destruction of digital information and records, see:

- IPC and National Association for Information Destruction (NAID) **Get Rid of it Securely to Keep it Private – Best Practices for the Secure Destruction of Personal Health Information** (October 2009)
- IPC Fact Sheet No. 10, **Secure Destruction of Personal Information** (December 2005)
- National Institute of Standards and Technology (NIST), **Special Publication 800-88, Guidelines for Media Sanitization** (December 2014)
- Government of Ontario, **GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices and Digital Storage Media** (March 2014)
- Communications Security Establishment Canada (CSEC) **Information Technology Security Guideline (ITSG-06) - Clearing and Declassifying Electronic Data Storage Devices** (July 2006)

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario