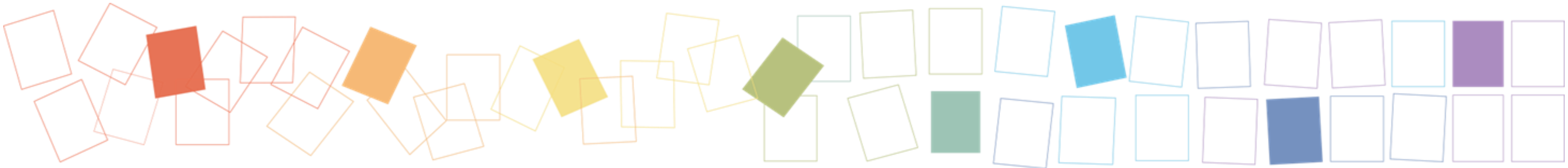

Managing your records outside the office

Do my recordkeeping responsibilities change when working outside the workplace?

No, the same basic principles apply to all workspaces, regardless if you work in a traditional office, at home, a public space or a mobile workspace. Government bodies need to create and keep complete and accurate records sufficient to document their decision-making and work activities. This applies to all types of government records, including documents in all formats and workspaces that provide the best evidence of government business activities, transactions, policy or decisions. These records must be managed in accordance with government records management policy and standards.

Responsibilities

Program areas are responsible for ensuring that there are:

- recorded policies and procedures
- defined roles and responsibilities
- appropriate recordkeeping systems
- ongoing training
- compliance monitoring programs

Employees are responsible for documenting their work by ensuring key records they create or receive are filed in their recordkeeping system.

Records Management Basics

File your records in an appropriate system

Wherever you work, it's important to routinely file your records in an appropriate system so that your co-workers have access to them. Records are inaccessible when left in individual email folders and on personal drives.

Using this approach will help you keep related records together and maintain complete files of specific activities, cases, or topics. This isn't possible if records are scattered across various individual email accounts, network drives and convenience files.

Appropriate recordkeeping systems include:

- **Local Area Network (LAN) / Shared Drives** structured according to *Administrative Records Classification System* (ARCS) and *Operational Records Classification System* (ORCS)
- **Enterprise Document and Records Management System (EDRMS)** Content Manager (formerly TRIM) is the government standard.
- **Line of business applications** (e.g. case management systems, SharePoint)
- **Physical filing system structured according to ARCS and ORCS**

Identify transitory information

When deciding what records you need to file, ask yourself: Is it transitory?

Transitory information is information of temporary usefulness that is needed only for a limited period of time in order to complete a routine action or prepare a final record. It can exist in any format or medium (paper or digital) and can be created and shared using a variety of technologies (e.g. email, social media, Skype for Business, SharePoint, wikis). Transitory information is not required for financial, legal, audit or statutory purposes and is not filed in the recordkeeping system. Transitory records are covered by the Transitory Records Special Schedule (102901).

To learn more about transitory information, review the Transitory Information Records Guide.

How can I protect government information when working away from the office?

If you work away from the office, you need to take extra precautions to ensure that sensitive government information is secure.

When working remotely:

- **Obtain your supervisor's approval** to work with confidential and/or personal information and take records outside the workplace.
- **Use the government network and/or a government-issued device** (e.g. laptop or mobile phone) whenever possible to store and access work information, rather than printing paper copies. (this reduces the risk of unauthorized disclosure or loss)
- **Limit the amount of confidential/and or personal information transmitted over email.**
- **Only disclose confidential information to authorized individuals** in a secure manner according to ministry approved processes.
- **Protect the information, particularly when working in a public environment** (e.g. ensuring that information is not viewable or accessible by others).
- **Physically secure government information when used outside the office** (e.g. locking and/or securing unattended devices to prevent unauthorized use or theft).
- **Destroy confidential records** either by returning them to the office and placing them into the locked disposal bins, or by running them through a cross-cut shredder that creates a fine shred ensuring confidentiality before putting the material in your recycle bins.
  If working in another government office, use the secure, locked disposal bins provided there.

When using a secure remote connection like VPN or DTS:

- **Do not download or save attachments to the local hard drive of a nongovernment device** as the files may contain confidential information.
- **Do not print any emails, attachments, or other documents when using remote access tools** (unless you are printing to a printer on the government network).

Also see relevant Office of the Chief Information Office (OCIO) documentation:

Working Outside the Workplace Policy provides direction on how to safeguard electronic and paper-based confidential information when working remotely.

Appropriate Use Policy sets out the policy requirements that all government employees must follow when accessing and managing government information (particularly confidential information); and using information technology (IT) resources.

Information Security Policy includes requirements for secure management of government information systems and devices.

Additional Information

Contact your Records Team or check out the rest of the Records Management website.