Western Australian Government

Records Management Advice

Working Remotely ('Work from Home')

For further information contact:
State Records Office of Western Australia
25 Francis St
Perth Cultural Centre
Perth WA 6000
+61 8 9427 3636

sro@sro.wa.gov.au

Document Version
This is a controlled document: Revision 1.0 as at 14 March 2022: Contact SRO for previous published versions.

Introduction

The State Records Office of Western Australia (SRO) is aware that State and local government employees work remotely, whether occasionally or for extended periods. Whatever the reason for remote work, it is important to remember your recordkeeping responsibilities are the same, whether it be at home, in another office, a mobile workplace or public space.

While working remotely all employees must continue to manage records of information (including data) appropriately and in accordance with your organisation's Recordkeeping Plan. This will ensure you, your organisation, and the public have the information they need now and into the future.

Employees should also be aware of and comply with their organisation's records management, information protection, and security policies for both hardcopy and digital information.

Key Points:

1. **Be aware!**

    - All information used in the performance of your duties, in whichever format, are records (including data) and your organisation has policies for its management
    - Understand your recordkeeping obligations in accordance with your organisation's policies, procedures and work instructions
    - Find out who in your organisation can help you understand your obligations – they'll know exactly what needs to be kept, where things should be kept and when they can be disposed of.
    - Records may be in any format including text messages, emails, letters, voice mail messages, social media posts and more.

2. **Capture records so they can be managed**

    - Ensure the data and information you create and use ('records of information') are captured appropriately and can be re-discovered, accessed and re-used as needed.

3. **Manage records so they:**

    - Can be re-used in an organised way in the appropriate systems
    - Are protected, preserved and stored in formats and conditions that ensure long term accessibility and usability (including copies, so they are as authentic, reliable and usable as the original source records from which they are created).
    - Are controlled securely to keep them safe from intentional or unintentional damage, unauthorised access, tampering or alteration.

4. **Don't destroy (or delete) records that need to be retained**

    - Your organisation will have formal policies, based in law and regulation, for dealing with disposing of records ('retention and disposal authorities')
    - Make sure to return control of information to your organisation (for instance, if you've worked 'off the network')

5. **Keep work and home records separate**

- Avoid using personal devices for work records, unless they are configured appropriately by your IT division.
- If, for some reason you must save a record on a personal device:
  - keep these on the device for the minimum time they're needed
  - keep them separate from your personal records, and
  - remove them from the device as soon as practicable - ensuring they are captured in a corporate system.
- Avoid using your private email, messaging apps or social media accounts for work
- Do not store the sensitive, personal information that your organisation uses on a personal device or personal information system (such as personal OneDrive, email, DropBox and the like).

6. **Managing records securely:**

- Become familiar with your organisation's Information Security Policy and complete the required information security training that your organisation requires.
- Keep records secure and not easily accessible except to those who need them.
- Only share records with those authorised to access them.
- Ensure all records, including copies, remain in the control of your organisation.
- Government records (including devices on which records of information are stored) must not be disposed of via household recycling or rubbish collections.

7. **The SRO recommends:**

- Organisations review their Remote Working and Information Security policies to ensure that record keeping expectations are clear and that expected remote based work activities can be performed in line with the Record Keeping Plan.
- Organisations align their Records Management and Information Security policies to ensure they address staff using Windows Virtual Desktop or Remote Desktop, vs accessing and downloading cloud-based information via their own equipment.
- Records and Information Management teams work closely with business areas to understand the practical needs of staff and provide guidance regarding best practice recordkeeping whilst working remotely.
- Records and Information Management teams implement processes to save information for those that are unable to access the official business systems and capture records as they normally would for example:
  - New record formats that need to be captured (e.g. capturing recorded teleconferences, or chats)
  - Consider workarounds that may need to be implemented
  - These changes be communicated to staff in coordination with other regular updates.

Employees may find the *'Records and Information Management Working Remotely Checklist'* useful to ensure they understand their record management responsibilities when working remotely (see **Annex A**, below). Tips and advice for record keeping for all employees is provided at **Annex B**.

Please make all staff aware of this advice.

References

Government of Northwest Territories, '*Enterprise Information Management Handbook' (revised December 2021)*, *'8300 Managing Government Records When Working Remotely*'(April 2020).

Government Records Office, Archives of Manitoba, *'Working Remotely and Recordkeeping Responsibilities'* (June 2020).

Government Records Service, Province of British Columbia, *'Managing your records outside the office'* (March 2020).

Public Record Office Victoria, *'Working remotely – recordkeeping responsibilities'* (April 2020).

Queensland State Archives, Records Connect Government Recordkeeping Blog, Recordkeeping & Working Remotely: 4 Tips to Make it Easier!

RELATED DOCUMENTS

Nil

ACTIVE DATE

March 2022

REVIEW DATE

March 2025

ANNEX A

Records and Information Management Working Remotely Checklist		
	Yes	No
General		
Have you been authorised to work remotely?		
Are you using your organisation's computer / laptop or other devices when working remotely?		
If using personal computing equipment, do you have permission to use it?		
Are you able to secure devices when they are not in use?		
Do you have external access to VPN and your organisation network?		
Can you protect your work from unauthorised access, use, disclosure, loss, destruction, or theft, including by members of your household?		
Do you understand your responsibilities under the *State Records Act 2000*, your organisations Recordkeeping Plan (RKP) and relevant Records and Information Management standards, policies and procedures?		
Do you know how to report missing, lost or damaged records, or devices containing records?		
Electronic Records		
Do you understand that personal email accounts should not be used to conduct government business?		
Do you understand how and where to save records?		
Do you understand how to transcribe government business conducted by text messaging or instant messaging and where to save it?		
If you print / copy records at home for ease of use, do you have a plan for returning the paper records to the office for secure destruction as soon as no longer required?		
Paper Records		
Do you have permission to remove paper records from the office?		
Do you understand the importance of protecting the privacy and confidentiality of paper records?		
Are you able to securely transport the records from the office to your remote work site?		
Are you able to securely store the records at home and prevent unauthorised access, use, disclosure, loss, destruction, or theft of the information, including by members of your household?		
Do you have a plan for the return of the paper records/physical files to the office as soon as no longer required?		

Source: *Enterprise Information Management Handbook* (Revised December 2021)

ANNEX B

RECORDKEEPING TIPS AND GUIDANCE FOR ALL EMPLOYEES

Creating good quality records (File notes etc.)
Sometimes important decisions or agreements will be made verbally, for example: in a meeting, over the phone, via text message, in voice mail messages, or some other way.

You should create a record of any verbal discussions that produce:

- agreements
- transactions
- decisions
- orders/directives
- formal advice or recommendations
- approvals and authorisations

Include:

- What was discussed
- The decisions or agreements reached
- Name of participants
- Who wrote the file note
- The date the discussion took place
- The date the notes were written

Capturing and storing records

- Use your organisation's official recordkeeping or business information systems to create and save records wherever possible. (e.g. EDRMS, CMS, Business Information System, shared drive and the like.)
- If you do not have access to official systems while working remotely, save them as securely as you can, and as soon as you have access move them into the official system.

Keeping Records Secure:

- Protect records from unauthorised access or modification.
- Meet security requirements set by your organisation.

Digital records:

- Lock your screen whenever you move away from it.
- If temporarily storing digital records on an agency approved USB storage device, lock the device away when not in use.

Physical records:

- Obtain permission before taking official registered files from your organisation.
- Ensure file locations are tracked within your organisation's official recordkeeping system.
- Protect physical files and documents from loss, theft, unauthorised access and damage when moving them between work and your remote location (particularly if using public transport).
- Keep physical files and documents in a designated area of your remote working location.
  - If possible, keep them in a locked area, particularly if they are confidential or contain sensitive information.
  - Do not allow anyone to view them
- Protect physical files and documents from damage (e.g. from liquids, food, dust, children, pets).
- Ensure the privacy of all personal or sensitive information is protected.

Tip: Immediately report any missing, lost or damaged records, or devices containing records, to your manager and the records management team.