

THE WOMEN'S HEALTH AND ACTION RESEARCH CENTER (WHARC)

Document Management Policy

1. Introduction

Documents are a vital part in the effective functioning of any organisation. We need documents on a short-term basis to help us to work consistently and productively and to keep track of progress in projects and activities. Creating standards for document management and ensuring that documents are created, managed and disposed of appropriately is a key part of good information management that will improve efficiency and mitigate legal and compliance risks (e.g. requirements relating to data protection, tax and employment). This must also be supported with the necessary guidance and training for staff to ensure they are confident document handlers.

2. Scope of the Policy

This policy applies to all members of the center and any individual creating or handling documents on the Center's behalf. The policy applies to all documents held in any format, including (but not limited to):

- Letters (digital and hard copy)
- Emails • Policies and guidance
- Meeting papers and minutes
- Reports • Contracts
- Presentations
- Official communications
- Photographs
- Audio recordings (other than voicemail messages)

Voicemail, text or instant messages do not constitute documents for the purposes of this policy, unless recorded or retained for specified purposes in accordance with legal requirements.

3. Objectives of the Policy

The Center must ensure that documents created in relation to its operations are being managed and maintained appropriately. This policy sets out standards and definitions to enable staff to create documents that:

- Meet the Center's internal requirements
- Enable the content of the document to be accessed, used and reused in a controlled and efficient manner

- Ensure the continuity of Center operations in the event of staff absence or emergency circumstances
- Are compliant with all regulatory and statutory requirements
- Enable the defence of the rights and interests of the Center and its stakeholders
- Are capable of providing evidence of a decision or operational process
- Are kept and maintained and stored in the most economical way consistent with the above objectives

4. Document management practices

The below list sets out practices that must be adhered to when creating and handling documents on behalf of the Centre:

- Documents must be clearly named (with date and version number if relevant) and stored in a structured manner
- Duplicate copies of documents must not be created unnecessarily
- Wherever possible, documents must be shared from their source location rather than attaching documents to emails
- Key documents (that others may require access to) must be stored in an appropriate shared filestore, i.e. not personal filestores (including desktop or device filestores)
- Copies of documents, whether digital or hard copy, must only be taken offsite when necessary (encrypted and password-protected removable storage or remote access via a secure network connection must be used whenever possible)
- Digital copies of document should never be emailed to a personal email account or stored on a personal cloud-based storage account
- Once a document is finalised, previous versions and drafts of documents should only be retained where entirely necessary e.g. for legal or audit purposes
- Appropriate metadata (such as title and tags) should be included at the point a new document is created to ensure it can be easily located and retrieved
- Any metadata contained in documents that have been created from previous versions or from templates created by another person should be deleted and/or updated
- Final copies of formal documents (such as policies or minutes) must be saved in PDF format
- As standard practice, the filename and storage location should be included in the footer of the document
- Formal documents that will be used and edited in the long term must include a document history or version control box to allow users to see the development of the document over time

- Regular audits (at least annual) of digital and hard copy information must be conducted to ensure that information is not retained longer than it is required

5. Naming Conventions and folder structures

A naming convention is a collection of consistent rules followed in naming documents, which should allow users to work effectively, ensure that files can be easily accessed by all who require access and to ensure that individuals are referring to and working on the correct document. The use of consistent naming conventions will improve efficiency by allowing staff to quickly identify the nature of the information contained within a document when searching through an archive or filestore. For further information, please see relevant guidance on naming conventions. Folder structures and names are also important in allowing the efficient retrieval of documents. The below principles must be followed when creating new folder structures:

- Folders must be clearly named by a relevant and meaningful subject area
- The names of individuals should only be used when creating a case file, i.e. not creating a personal folder in a shared filestore
- Top level folders must be kept to a minimum
- Ideally, file structures should not exceed six levels of subfolders
- Appropriate access levels must be assigned depending on necessity to access the documents contained within the folder

6. Information Classification Scheme

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Open	Available to all authenticated members of WHARC staff
Confidential	Available only to authorised and authenticated members of staff
Confidential & Sensitive	Access is controlled and restricted to a small number of named, authenticated members of staff
Secret	Known only to a very small number of authenticated members of staff

While it is not mandated that all documents and records are marked with the relevant classification, it is good practice to include the classification in the document header or footer, or by way of a watermark (on a digital copy) or stamp (on a hard copy), to ensure that users and recipients are aware of the potential sensitivity of the content.

7. Digital Preservation

Where documents or records are either “born digital” or where hard copies are digitised, WHARC will ensure that there are appropriate standards and guidance in place to ensure that records of permanent or continuing value remain accessible and preserve their integrity for as long as required, accounting for changes in IT software and hardware. Adherence to these standards and guidance will safeguard the authenticity and integrity of digital materials in the long term and will allow the storage of digital materials safely through adoption of security mechanisms appropriate to each classification of material.

8. Destruction

All documents must be subject to action proscribed in WHARC’s Records Retention Schedule, which may be destruction, at the end of the assigned retention period unless such period has been suspended on learning of an actual or reasonably anticipated claim, audit, investigation, subpoena or litigation asserted or filed by or against WHARC. IAOs and IAAs should periodically determine whether any documents under their control should be destroyed in accordance with the Records Retention Schedule

9. Policy review and Ownership

This policy will be reviewed and amended as required, and at least every three years the board.

Policy Approved By:



Dr. Wilson Imongan
ED. WHARC