



Document Management Policy	
Publication date: 1 May 2018	Applies to: All members
Responsible person: Secretary	Scheduled review date: At least once every three years as determined by the Committee
Approved by: Committee meeting 9 April 2018	Author: Secretary

INTRODUCTION

U3A-ACT Inc. Objects and Rules require the Committee to *control and manage the affairs of the association* (Rule 14) and identify that the Secretary must *keep in his/her custody or under his/her control all records, books and other documents relating to the organisation* (Rule 20). The Rules also make provision for the responsibilities of the Treasurer to *keep correct accounts and books showing the financial affairs of the association* (Rule 21, 1(b)).

PURPOSE

This policy is designed to set out the arrangements for managing our documents in order to meet the requirements of our governing Objects and Rules and legislation, and to provide for orderly governance and retrieval of documents within the association.

DEFINITIONS/KEY WORDS

U3A-ACT Inc. Documents: Those materials which need to be kept for the proper conduct of U3A-ACT Inc. business or which are official publications of the association. These include:

1. materials required to be kept by law or under our *Objects and Rules*
2. Committee approved documents
3. Official publications
4. Operational procedures
5. Key emails that are part of official correspondence (eg an email to the Treasurer that authorises the payment of a contractor)
6. Manuals
7. Minutes of sub-committees and working groups where these are kept
8. Key images, video and sound recordings relevant to U3A-ACT Inc.'s history.

Materials excluded from this definition: materials that constitute working drafts, notes, musings, papers in development. These do not represent an officially endorsed position or view of the association and cannot be represented as doing so. Materials we do not need to keep so that we can learn from our experience.

Such materials may be shared with other members provided the Privacy Policy is not contravened.

Course materials are assigned to this category as they belong to individual course presenters, not to U3A-ACT Inc.

Centralised electronic repository (CER): the arrangements approved from time to time by the Committee for electronic storage of U3A-ACT Inc. documents. At the time of introducing this policy the approved CER arrangement is Google Drive.

Document Authoriser: a person authorised under this policy to give permission for a document to be kept as an official record of the association and for it to be filed in the CER.

Document Management Officer (DMO): the person appointed by the Secretary to perform the duties of the Document Management Officer as described in this policy. Where Assistant Document Management Officers are also appointed by the Secretary they may perform any of the functions assigned to the Document Management Officer as agreed with the Document Management Officer.

POLICY

1. This policy applies to U3A-ACT Inc. documents as defined above.
2. U3A-ACT Inc. documents are generated by:
 - 2.1. committee processes
 - 2.2. external contracts and commitments (eg insurances)
 - 2.3. the work of the management coordinators and their teams
 - 2.4. member activity when it relates to any documents encompassed by the definition of U3A-ACT Inc. documents
3. New or amended documents may only be added to the CER if they have been authorised by a person approved as a Document Authoriser.
 - 3.1. A Document Authoriser may advise the Document Management Officer that he or she authorises another person or persons to be Document Authoriser for parts of the CER for which the first Document Authoriser has responsibility.
4. U3A-ACT Inc. documents have authority that can be seen on the face of the document
 - 4.1. Every document (as defined in this policy) should show who authorised it, if it was not the committee, the position that person held when they authorised it; its access classification and the date on which it was authorised
 - 4.2. The Document Authoriser is responsible for providing the document to the Document Management Officer for filing in the CER.
5. The official copy of all documents is held in the CER.
 - 5.1. Documents which do not originate in electronic document format should without exception be converted to an electronic document form and held in the CER.
 - 5.1.1. The originals of these documents should then be destroyed.
 - 5.1.2. In exceptional circumstances some items (eg contracts or auditors' reports) may also require filing as hard copies
 - 5.1.2.1. The Secretary will decide which documents should be held as hard copies in addition to the electronic form

- 5.1.2.2. Where a hard copy document is retained for official purposes the CER copy should be annotated to say where and how the hard copy can be found.
6. The CER is managed by the Document Management Officer reporting to the Secretary in accordance with this policy. The Document Management Officer will
 - 6.1. add, amend, retain or delete documents in the CER in accordance with this policy and as requested by Document Authorisers
 - 6.1.1. The Document Management Officer cannot make changes or deletions to documents, files or folders without authorisation from a Document Authoriser or the Secretary.
 - 6.2. ensure documents are filed in the appropriate place according to a documented filing system
 - 6.3. manage access to the CER on behalf of the committee
 - 6.4. ensure that regular and appropriate back-ups are undertaken of the whole CER
7. All documents will be classified into four categories of access:
 - 7.1. Available to the general public (category G)
 - 7.2. Available to all members (category M)
 - 7.3. Available to current committee members only (category C)
 - 7.4. Available to a person or persons approved by the Committee or the Document Authoriser (category R)
 - 7.5. Documents may fall into both category C and category R at the same time.
8. Documents can be accessed according to each category
 - 8.1. Category G are accessible as read only documents from the U3A-ACT Inc. public website.
 - 8.2. Category M are accessible as read only documents to all members by methods determined by the Committee from time to time depending on the technical infrastructure available.
 - 8.2.1. the committee will endeavour to ensure that hard copies of documents are available on request at our offices to members who have an entitlement to view Category G and M documents and do not have access to the internet
 - 8.2.1.1. The Committee retains the right to limit hard copy access under 8.2.1 if demands from members exceed our capacity to provide the service.
 - 8.3. Category C are accessible as read only documents to all committee members from the CER
 - 8.4. Category R are accessible as read only documents from the CER and access is assigned to specific members identified by the Committee or by the Document Authoriser in the area of the filing structure concerned.
 - 8.4.1. The relevant Document Authoriser must advise the Document Management Officer of the names of members who are to have access to the documents classified as R. The Document Authoriser is also responsible for ensuring that the Document Management Officer has up-to-date information on those who need access and those for whom access should be removed.

8.4.2. This category will generally hold sensitive materials (eg matters relating to membership, complaints, results of investigations, business in confidence documents.) or relate to a specific volunteering area (eg Banking Volunteers)

8.4.2.1. Until an integrated IT system is available some category R documents (such as membership information) may continue to be held on databases accessed on designated machines which are secured in U3A offices and to which there is restricted access.

9. Nothing in this policy negates the rights of members to inspect books as set out in Rule 44 of the Rules.

10. Documents may only be added to the CER, moved within it, or deleted from it by those who are approved to do so by the Committee.

10.1. This will be the Secretary, and the Document Management Officer, unless decided otherwise by the Committee.

10.2. The Document Management Officer may delegate any of his/her duties to Assistant Document Management Officers working under the Document Management Officer.

11. Documents should be retained or securely destroyed according to timeframes dictated by each of the specific laws, policies or Committee decisions that apply to the document or classes of documents.

11.1. The default retention period will be seven years.

12. This policy does not preclude volunteers printing hard copies of documents to assist in their day to day operational activities.

SOURCES

- ACT Associations Incorporation Act 1991
- Australian Privacy Act 1988
- Australian Charities and Not for Profit Commission (ACNC) Act 2012 (Cwth)
- ACNC record-keeping requirements (see http://www.acnc.gov.au/ACNC/Manage/Record_keeping/ACNC/Edu/Record_Information.aspx?hkey=5f579f6a-6b9e-49f0-aa70-de27abdd5efd)
- The Australian Privacy Principles
- U3A-ACT Inc. Objects and Rules

REFERENCES

www.records.nsw.gov.au/.../documents

http://w3.unisa.edu.au/safetyandwellbeing/SMS/procedures/document_control_and_record_management.pdf

<http://www.naa.gov.au/records-management/strategic-information/information-governance/key-documents/policy.aspx>

<https://www.maddocks.com.au/reading-room/document-retention-and-destruction-in-australia>