



## Document Storage Policy and Procedures

<b>Title</b>	Document Storage Policy and Procedures	<b>Policy No</b>	PN-0016
<b>Version</b>	2	<b>Date of Approval</b>	02/06/2023
<b>Pillar area</b>	Governance	<b>Schedule review date</b>	2025

### Introduction

As a national organisation with Directors and staff located nationally, it is essential for AusDBF to have an electronic structure where documentation can be centrally saved and accessible for all Directors and staff to retrieve.

Whilst working or volunteering on behalf of AusDBF all documentation remains the intellectual property of AusDBF. A copy of all documentation must be retained and saved on AusDBF Sharepoint.

All communication to AusDBF Members to be distributed via AusDBF Business Services to ensure a copy of communication is kept on file.

AusDBF hardcopy documents (mostly historical) are kept in a storage warehouse. The documents are stored in weatherproof boxes and labelled.

### Purpose

Electronic document retention management needs to meet multiple objectives:

1. That document retention does not materially degrade IT system performance.
2. That important documents remain accessible for operational purposes.
3. That legal document retention requirements are met; and
4. That *Privacy Act* obligations to delete certain personal information is complied with

### Administration

AusDBF uses office365 for its software with Sharepoint (*intranet site*) and Teams for the document storage. AusDBF has a number of licenses with office365 which are allocated to Board Directors, Staff and volunteers as required. The licenses provide access to Sharepoint, Teams and OneDrive.

AusDBF has set-up '**Teams**' for each of its Committees, Commissions, and working groups to enable easy communication with each other and a central folder for saving and accessing documents.

### Responsibilities

It is the responsibility of AusDBF Business Services to ensure that:

1. staff and volunteers are aware of this policy
2. any breaches of this policy are brought to the attention of the AusDBF Board and dealt with appropriately
3. It is the responsibility of all employees and volunteers to ensure that their usage of email documentation storage conforms to this policy.
4. All AusDBF communication which includes, though is not limited to, confidential management information, employee-related information, and project-related correspondence is saved securely and according to naming convention.

PROCEDURE

Sharepoint (AusDBF intranet) - <https://ausdbf.sharepoint.com/>

This is the platform where AusDBF archives all historical documents and final approved documents are saved.

The ‘document library’ located on the left is in alphabetical order and filed under subjects. Within each ‘document library’ separate folders are set-up generally in calendar or financial years or specific topic. For

example: -

AusChamps > 2020 AusChamps (ACT) > then folders or files as relevant

AusDBF Committees > AusChamps Review > folders or files as relevant

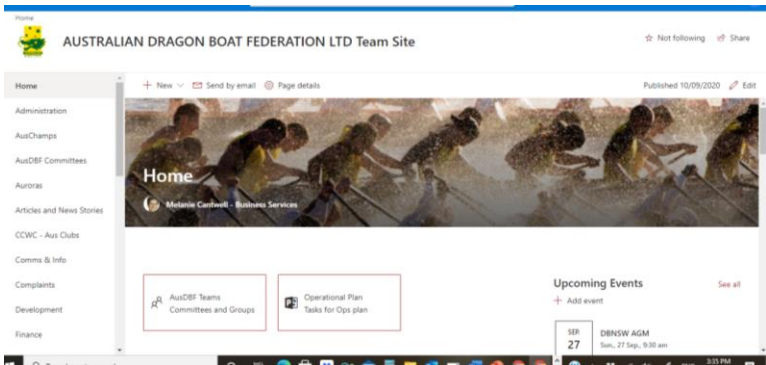


Figure 1: AusDBF intranet and Document Library listed on the left

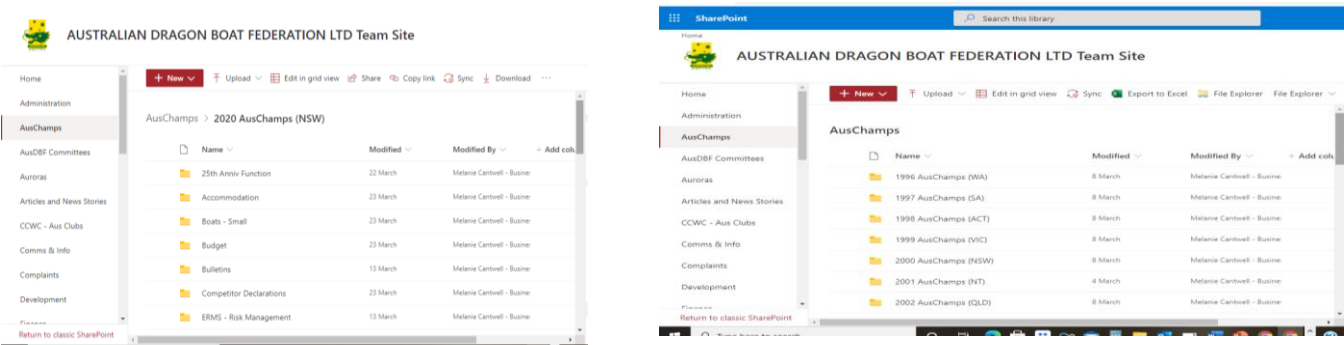


Figure 2: Folders with each Document Library

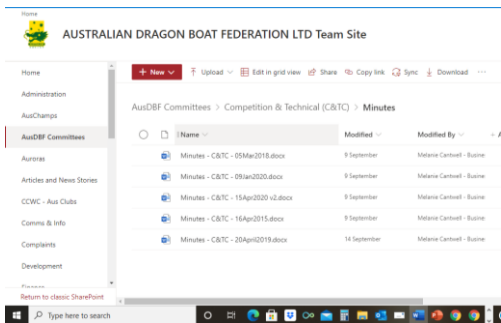


Figure 3: Files within each Folder

## **Saving Documents**

1. Final version of documents must be saved in word, excel etc in addition to PDF to enable future edits to be made
2. Each document library has its own 'Archived Folder' where previous versions of relevant documents can be stored for future reference
3. Current and approved versions of documents are saved in the named folders
4. Once a policy or **relevant** document has been updated, the previous version is moved to the 'Archived Folder'
5. New or revised documents must be uploaded to the website and replace previous versions
6. Where possible documents should be saved per calendar year for example:
  - a. AusChamps folders have been created per year, with further sub-folders created
  - b. Auroras folders have been created per year (campaign) with further sub folders created
  - c. Finance folders have been created per financial year
  - d. Memos and Updates have been created per calendar year
  - e. Meetings and Minutes have been created per calendar with further sub-folders created
7. Other folders have been set-up per category or topic for example:
  - a. AusDBF Committees with sub-folders created for each committee
  - b. Development with sub-folders create for coaching, race officials, Oceania etc
  - c. Policies-Procedures with sub-folders created

## **What types of document should be kept?**

- Final versions
- Communications – such as correspondence with members, employees, contractors etc, external organisations
- Legal and financial
- Quotes
- Historical

## **What types of documents can be deleted?**

- drafts
- non-relevant

## **Access to Folders and Files**

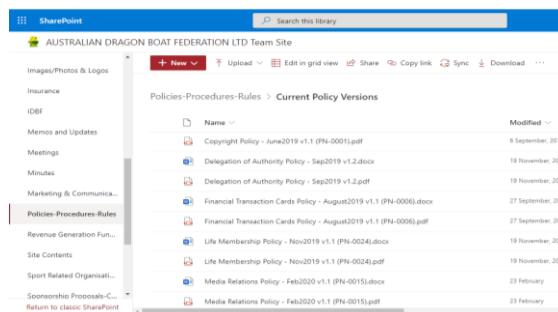
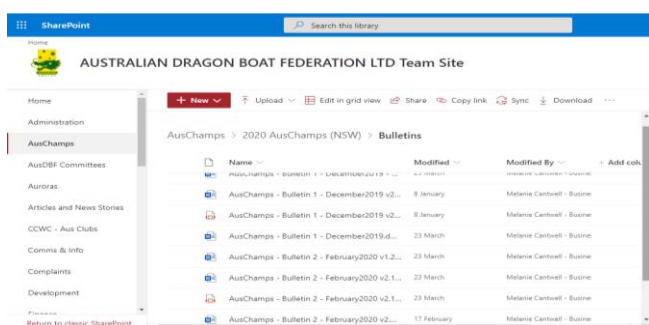
1. All folders will have access granted depending upon the need. People who have responsibility for the contents of that folder will have READ access, those who have rights to view the contents will have view access only.
2. People who have no rights to see a folder will not have access at all.
3. It is the responsibility of each Director and employee/s to save documents in the correct folders using the stipulated naming conventions

## **Length of time to keep documents**

- Financial and legal – save for 7 years
- General – 5 years
- Documents containing historical information on AusDBF and dragon boating should be kept

## **Procedure for when Board Directors retire, or employees resign**

It is the responsibility of Directors and employees to ensure they transfer and save any documents they have worked on from their personnel drive to the AusDBF Sharepoint drive according to filing and naming convention.



## Naming Conventions

1. Minutes must be saved as topic-Committee-date-version  
For example, 'Minutes – C&TC – 2020-05-28 v2' For example, Policy name – date – version- (PN-xxxx)

Figure 4: example of saved documents naming convention

2. General documents
  - a. Handbooks, Regulations, documents with front covers should be created and updated as follows –
    - i. 'edition' = for example Edition 9 was approved in 2020. Edition 8 was approved in 2019
    - ii. If updates are made to the document throughout the year they would be noted as 9.1, 9.2 etc
    - iii. 'versions' (v9) = would be used as drafts while the document is being worked on to keep track of latest version. For example – Edition 9 – drafts be noted as v9.1, v9.2, v9.3
    - iv. When draft has been finalised and ready for Board approval FINAL should be included for example – Competition Rules & Regulations – Edition 9 – 2020-Oct-10 – FINAL
    - v. 'approved' = date of the Board meeting document was signed off
    - vi. Pages should be included on all documents in bottom footer right hand side – for example 2 of 3



Figure 5: sample of front cover



Figure 6: sample of footer

- b. Policies
  - i. Policies and guidelines for consistency are to utilise the corporate template
  - ii. 'version' refers to the latest version approved and published by AusDBF Board
  - iii. 'draft' should be noted as 2.1, 2.2 whilst the document is being reviewed.
  - iv. When draft has been finalised and ready for Board approval FINAL should be included for example Integrity & Match Fixing Policy – 2020-Aug v2 FINAL (PN-0026)
  - v. Policy number should be included in title to help keep track of numbers

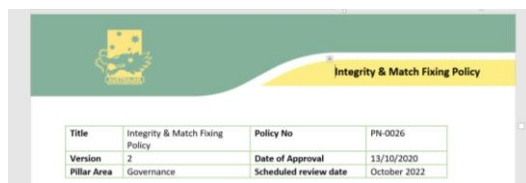


Figure 7: Sample of policy header

### c. Use of Logos and templates

- AusDBF officially trademarked their logo and Aurora's logo in 2019, all documents must include these updated logos
- Depending on background of document, the IDBF or Oceania may be deemed as important to be included
- AusDBF corporate templates include – letter head, memo, policy, power-point

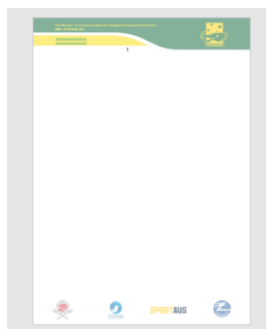


Figure 8: Letter Head template



Figure 9: Memo template



Figure 10: Policy template

## Teams

Teams is where 'collaboration' occurs. Teams can communicate with each other via 'posts' and share and collaborate on working documents via 'files'

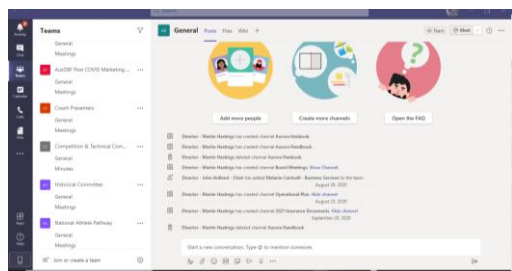


Figure 11: Posts Screen

For each 'Team' AusDBF has created 2 channels:

### 1. General

Folders can be created for specific topics. Each Committee already has Charter & Contacts folders created. Drafts for documents are saved here. Final versions are then forwarded to AusDBF for approval where they are saved in Sharepoint.

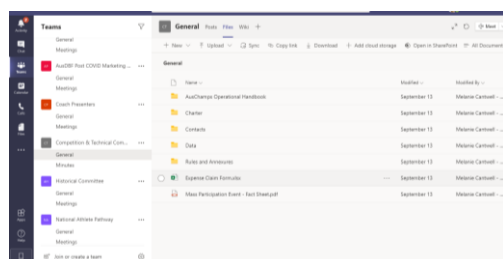


Figure 12: General 'Files' channel

## 2. Minutes

Each meeting will have a folder created using the naming convention YYYY-MM-DD. Saved in each folder will be agenda, minutes, papers for discussion for that meeting

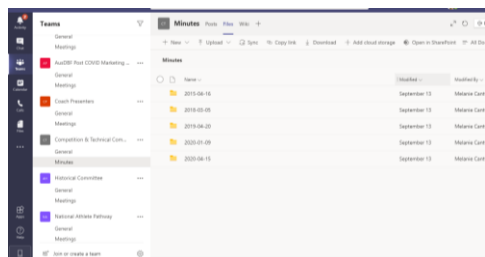


Figure 13: Meetings 'Files' Channel

**All documentation which was obtained or created whilst under AusDBF must be saved to AusDBF Sharepoint folders and any personnel information obtained about members must be deleted from ALL personnel computers prior to last day with AusDBF.**

## APPENDIX – background information

### Personal Information

- Australian Security Investment Commission (*ASIC*) requires companies to keep records for seven (7) years from the end of the last financial year they relate to, or longer if they show a transaction that covers more than one of the company's accounting periods.
- The Fair Work Ombudsman (*FWO*) requires you to keep employee records for seven (7) years
- The Australia Tax Office (*ATO*) requires records to be kept for five (5) years
- Records for ASIC and ATO must be kept in writing, either on paper or electronically, in English and all transaction explained
- All business in Australia are required by law to keep records and documents related to how their business operates. Records which businesses need to keep are financial records, legal records, employee records, policy and procedures, other business records.
- Australian Privacy laws apply to the collection, use and storage of personal information. Personal information is information that could identify whom someone is. Some examples are name, address, phone number, date of birth and bank account details.
- Electronic copies of records are now generally accepted by government departments such as ASIC and the ATO. Electronic copies must be a true and clear copy of the original. Records kept on a computer or device must allow access (including passwords), be backed up in case of computer failure, allows the control of information that is processed, entered and sent.

### Privacy Act 1988 (Cth)

Under the Australian Privacy Principles implemented in accordance with the *Privacy Act 1988* (Cth), an APP entity (ie an entity that is obliged to comply with the Australian Privacy Principles) must take such steps as are reasonable in the circumstances to destroy personal information, or to ensure that the information is de-identified, if the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity. The *Privacy Act* only applies to information about an individual (ie a human) it does not apply to information about entities. Furthermore, determining whether the entity has any continuing need for the information is based upon uses that are permitted under the *Privacy Act*, not all possible uses to which the entity may want to put the information. However, this obligation is expressly subject to any obligation at law to retain the information so that an obligation to retain overrides this obligation to destroy

### Destruction of evidence

Various state and territory laws criminalise the destruction or concealment of a document that is likely to be required in evidence in a legal proceeding.

In Victoria under the *Crimes Act 1958* (Vic) s 254, it is an offence to destroy, conceal or render illegible such a document, or to expressly, tacitly or impliedly authorise another person to do so. This applies to legal proceedings that have been commenced or may be commenced in the future.

The law in Victoria represents a high-water mark for such obligations. By contrast, the equivalent offences in the other states require an element of intention to affect judicial proceedings. As such, compliance with the Victorian law should determine the standard complied with by any entity that operates nationally (or otherwise in Victoria).

In New South Wales under the *Crimes Act 1900* (NSW) s 317, it is an offence to suppress, conceal or destroy anything knowing that it is or may be required as evidence in any judicial proceeding, with the intent to mislead any judicial tribunal in any judicial proceeding.

In Queensland under *The Criminal Code* s 129, it is an offence to damage evidence, knowing it is or may be needed in evidence in a judicial proceeding.

In South Australia under the *Criminal Law Consolidation Act 1935* (SA) s 243, it is an offence to conceal or destroy anything that may be required in evidence at judicial proceedings with the intention of influencing a decision by a

person whether or not to institute judicial proceedings or to influence the outcome of judicial proceedings (whether proceedings that are in progress or proceedings that are to be instituted at a later time).

In Tasmania under the *Criminal Code Act 1924* (Tas) s 99, it is an offence to willfully destroy or conceal any evidence, or anything likely to be required as evidence in any judicial proceeding, with intent to mislead any tribunal in any judicial proceeding or to pervert or defeat the course of justice.

In Western Australia under The Criminal Code s 132, it is an offence to willfully destroy or render illegible any document that is or may be required in evidence in a judicial proceeding, with the intent to prevent it from being used in evidence.

.