



Email Retention Policy and Procedures

Title	Email Retention Policy and Procedures	Policy No	PN-0018
Version	2	Date of Approval	02/06/2023
Pillar area	Governance	Schedule review date	2025

Introduction

The rise to predominance of electronic communication mandates electronic message management systems comparable to existing hard copy filing systems.

Employees and volunteers of the Australian Dragon Boat Federation (*AusDBF*) have no rights in any material, electronic or otherwise, created by in the course of their employment or appointment to *AusDBF*.

Purpose

Email retention management needs to meet multiple objectives:

1. That email retention does not materially degrade IT system performance
2. That important emails remain accessible for operational purposes
3. That *Privacy Act* obligations to delete certain personal information is complied with

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

Email addresses

To ensure continuity of information AusDBF uses common email addresses which allow the ability for communication and transference of information as easy as possible.

What types of emails should be kept?

- Emails containing decisions or approvals
- Emails containing matter related to legal obligations (e.g. finance, insurance, constitution) -
- Emails containing historical significance to AusDBF
- Emails creating or recording permanent legal relationships (sponsorships/partnerships)
- Emails containing information with regards to specific projects

PROCEDURE - Email etiquette

Length of time to store emails

- Financial and legal – save for 7 years unless stored elsewhere
- General – 5 years unless stored elsewhere

What emails can be deleted

- Copied into emails, don't keep them originator of email will keep them
- Every director every quarter should purge emails

Filing of emails

- Calendar year (Jan-Dec)
- Strategic Pillars
 1. Governance
 - a. Board Meetings
 - b. Policies
 - c. AusDBF Members
 - d. AusDBF Committees
 - e. Safety & Risk
 - f. Finance
 2. Development
 - a. Coaching Courses
 - b. Race Official Course
 - c. Sweep Course
 - d. Other
 3. Events
 - a. AusChamps
 - b. Other
 4. High Performance
 - a. Auroras
 - b. CCWC

Procedure for when Board Directors retire, or employees resign

It is the responsibility of Directors and employees to clean-up their emails prior to their last day with AusDBF. This is to ensure information is easy to find when the email address is transferred to the next person and the next person using the email address does not have to spend valuable time sorting and storing the previous users emails.

1. All emails in the 'inbox' should be filed or deleted
2. All emails in the 'sent box' should be filed or deleted
3. All emails in the 'deleted box' should be deleted

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 Policy 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.