Connectivity
Traumatic Brain Injury Australia

DECEMBER, 2020

DATA MANAGEMENT POLICY

Contents

Connectivity
Traumatic Brain Injury Australia

Purpose of the Policy

Vision TBI's information is a corporate asset. It is valuable both for ongoing operations and in providing background to business decisions and activities. Vision TBI is therefore committed to creating and keeping accurate information.

Scope

This policy:

- sets out to explain the expected information management practices, processes and systems that will support information being managed as an asset
- explains the benefits of good data management
- Applies to all staff, board and committees of Vision TBI
- Applies to all business information created including documents, email, voice message, minutes, audio-visual material and business system data.

Background

This policy seeks to complement other Vision TBI policies including:

- Communications Policy
- Crisis Communications Policy
- Social Media Policy
- Privacy Policy

Creation and Maintenance of Information

Business information must be created and captured by everyone subject to this policy. Business information created should provide a reliable and accurate account of business decisions and actions. Information should include all necessary detail to support business needs, including names, dates and time, and other key information needed to capture the business context.

It is our responsibility to create records that support the work that we do along with practical reasons for managing our information, including:

- To provide evidence
- Demonstrate accountability
- Identify and minimise risk
- Make informed decisions
- Preserve our history

Good records practice involves ensuring that our information it:

- Stored in the appropriate places
- Names and organised
- Protected

- Controlled and kept for set periods of time

Destruction of Information

If information is out of date it should be stored in an archive system, and disposed of only after an appropriate retention period, and if it is not required for historical purposes.

Some information may be destroyed in the day to day business this includes draft meeting notes, draft versions of documents not needed for future use, etc.

Staff should be aware that the unauthorised destruction of material may lead to a range of risks including:

- an inability to comply with regulatory and legislative responsibilities such as the Freedom of Information Act 1982 and the Privacy Act 1988
- an inability to provide access to information requested by legal discovery action
- damage to organisational reputation

It is recommended that a retention and destruction schedule is created so staff and the Board are aware of the recommended management periods of information.

Access to Information

Staff should readily be able to access information on the shared drive. This is a corporate resource which all staff may have access to with the exception of classified information such as:

- Individual staff or client private information
- Sensitive material such as medical records

When handling information, staff are reminded of their obligations under the APS Values and Code of Conduct, the Crimes Act 1914 and Public Service Regulations.

Transfer

Transfer of information should take place in the event of staff handover, in which case information should be passed to the CEO or the newly recruited member of staff.

Review

The Policy should be reviewed at the end of 2021.