INFORMATION SECURITY POLICY

1. Intent and Scope

(a) This information security policy (**policy**) provides the basis of information security management within the Childhood Dementia Initiative (**CDI**).

(b) This policy aims to balance the following priorities:

(i) Meeting the CDI's legislative requirements.

(ii) Keeping data and documents confidential as required by the CDI and its stakeholders.

(iii) Ensuring the integrity of the CDI's data and IT systems.

(iv) Upholding the CDI's reputation as a trusted recipient of data.

(v) Maintaining storage and back-up systems that meet the needs of the CDI and its employees, contractors, volunteers, and anyone else who may have any type of access to the CDI's systems, software, hardware, data and/or documents (collectively referred to as the **Participants**).

(vi) Ensuring the CDI's compliance with relevant data protection and privacy regulations, including but not limited to the *Privacy Act 1988* (Cth) and the *Australian Privacy Principles*.

2. Responsibilities

(a) This policy applies to all Participants who are given access to the CDI's systems, software, hardware, data and/or documents.

(b) All Participants are responsible for protecting business information and systems. Where there is any doubt about the security of any action, the Participants should take a cautious approach and avoid any potential risks.

(c) The Information Security Officer/ Operations Manager is responsible for implementing this policy.

3. Authorisation and Access

The CDI's managers should exercise caution when:

- Sharing information and documents with the Participants.
- Authorising the Participants to enter and control information systems.
- Giving the Participants access to information systems.

As a general rule, managers should follow a need-to-know basis. If there is any uncertainty regarding how information and documents should be shared, contact the Information Security Officer at info@childhooddementia.org

4. Password and Authentication Requirements

(a) To avoid the Participants' work account passwords being compromised, these best practices are advised for setting up passwords:

(i) Passwords set up by an administrator must be uniquely and randomly generated, then immediately changed by the user.

(ii) Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols).

(iii) Do not write down password and leave it unprotected.

(iv) Do not exchange credentials when not requested or approved by supervisor.

(b) Change passwords when there is any possibility that an existing password may have been compromised.

(c) We encourage the use of a password management tool, whether integrated into a mobile app or an internet browser.

(d) Multifactor authentication tools should be used where possible.

5. Email Security

Emails can contain malicious content and malware. In order to reduce harm, the Participants should employ the following strategies:

(a) Do not open attachments or click any links where content is not well explained.

(b) Check the email addresses and names of senders.

(c) Search for inconsistencies.

(d) Block junk, spam and scam emails.

(e) Avoid emails that contain common scam subject lines such as prizes, products and money transfers.

(f) Where an email requests financial payment, confirmation of password, or prompts to login to a CDI system, extreme care should be taken to ensure that it is genuine, such as by calling the sender.

If the Participant is not sure that an email, or any type of data is safe, the Participant should contact the Information Security Officer info@childhooddementia.org

6. Device Security and Using Personal Devices

(a) Logging in to any work accounts on personal devices such as mobile phones, tablets or laptops, can put sensitive data at risk. However, if this cannot be avoided, the Information Security Officer advises that Participants adopt the precautions in clause 3(b).

(b) The Participants are recommended to follow these best practice steps:

(i) Keep all electronic devices' passwords secure and protected.
(ii) Logging into accounts should only be performed through safe networks.
(iii) Install security updates on a regular basis.
(iv) Upgrade antivirus software on a regular basis.
(v) Never leave devices unprotected and exposed, particularly in public spaces.
(vi) Lock computers when leaving the desk.
(vii) When accessing trusted external systems, all applicable guidelines must be complied with.

(c) It is recommended that any Internet of Things (**IoT**) devices are kept segregated from the CDI systems unless they have been approved by an IT specialist for use.
(d) The Participants must not use unauthorised devices on their workstations, unless they have received specific authorisation from the Information Security Officer.
(e) Any devices deemed no longer suitable for use must be disposed of in a secure way to ensure all information is permanently removed.

7. Transferring Data

Data transfer is a common cause of cybercrime. The Participants should follow these best practices when transferring data:

(a) Avoid transferring personal information such as user data and employee information (this includes anything that can or may identify an individual including first name, last name, age, address and email address).
(b) Adhere to the relevant personal information legislation including the Australian Privacy Principles.
(c) Data should only be shared over authorised networks.
(d) If applicable, destroy any sensitive data when it is no longer needed.

8. Working Remotely

When working remotely, all the information security policies and procedures must be followed.

9. CDI Systems

(a) When accessing the internet from any system set up by the CDI:
(i) Participants must use the standard process and not bypass any security measure.
(ii) Reasonable care must be taken in relation to when downloading documents and transmitting data over the internet. Access only trusted websites.

(b) When accessing accounts on the CDI systems:
(i) User accounts on work systems are only to be used for the business purposes of the CDI and not to be used for personal activities.

(ii) Participants are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Participants are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of the CDI.

(iii) Participants must not purposely engage in any activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to CDI systems for which they do not have authorisation.

10. General Security Requirements

(a) Participants must not install unauthorised software. The CDI may at any time introduce a whitelist of approved/trusted programs. If this occurs then only these programs may be used by the Participants.

(b) Participants should stay up-to-date with any other CDI-wide recommendations, such as recommended browser settings.

(c) Participants should perform daily backups of important new/changed data, software and configuration settings.

(d) Participants must not attempt to turn off or circumvent any security measures.

(e) Participants must report any security breaches, suspicious activities or issues that may cause a cyber security breach to the Information Security Officer immediately and await their instructions regarding the appropriate response to the breach.

11. Other Companies Policies

This Policy must be followed in conjunction with the CDI's Privacy Policy which can be accessed here.

12. Training

All Participants must maintain working knowledge of basic information security protocols. All new Participants will be given training on information security.

13. Disciplinary Action

If this policy is breached, one or more of the following disciplinary actions will take place:

(a) Incidents will be assessed on a case-by-case basis.

(b) In case of breaches that are intentional or repeated or cases that cause direct harm to the CDI, Participants may face serious disciplinary action, including termination of your employment, engagement or services.

(c) Subject to the gravity of the breach, formal warnings may be issued to the offending Participants.

14. Review

The CDI will periodically review this policy and update as required to ensure the continued security of the CDI. It is important for those to whom this policy applies to stay up-to-date with changes to this policy, as this is a rapidly-changing area of technology.