Information Security Policy

Scope
This policy applies to Brook RED Community Members/NDIS Participants, Nominated Support People, board members, employees, volunteers, and students on placement.

Purpose
To ensure that all personal and private information collected about individuals to whom Brook RED delivers services is appropriately handled at all times.

Principles
Brook RED understands the value and importance of personal and organisational information and wishes to treat it with the utmost respect and care at all times.

Policy

Personal information
All personal information, including that of Community Members/NDIS Participants and employees, must be:

- Stored securely with reasonable security precautions against misuse or unauthorised access (e.g. electronic information should be password protected, hard copies stored under lock and key)
- Readily accessible but only on a need-to-know basis
- Retained for the required time (7 years)
- Destroyed securely when no longer required
- Not shared with any third parties without correct consent

General information security precautions

- Access to all personal information is strictly based on a need-to-know basis
- When sending group emails, use the “BCC” filed rather than the “To” field so email recipients cannot see other recipients email addresses
- Always password locked computers when unattended (shortcut to password lock a Windows computer is “Windows key + L”
- Operating system updates (also called “patches”) must be installed promptly after they become available
- Active anti-virus software must be installed and kept up-to-date on all computers
- Internet modem routers must have security (ie firewall) enabled and must have a strong admin password
- WiFi networks must have strong passwords to gain access
- A VPN is used where appropriate
- Only download or install software from trusted sources
- Mail servers should be configured to use encryption
- Computers should be configured so admin rights are restricted to management
- When an employee leaves, their access to the organisations computer network and email systems is removed promptly

Information Security Policy

Information Technology (IT) System

- Brook RED have implemented Careview as the IT System for managing participant information for some specific programs
- In addition to the general information security precautions indicated below, Brook RED will ensure:
  - Each user has an individual user login to the Careview system
  - Each user will be provided with training in the use of the Careview system and their obligations with regard to managing personal and private information

Passwords

- All computers which store or access personal information require unique and strong passwords to gain access
- Passwords must not be shared or reused between computers, users, or different applications
- Passwords should not be left written on paper left lying around
- Passwords should be regularly changed i.e. every three months
- Always use strong passwords with a minimum of 8 characters which include a combination of:
  - Lower case letters
  - Upper case letters
  - Numbers
  - Symbols
- Do not use easy-to-guess passwords such as “12345”

Avoiding scams and ransomware

- Do not pay the ransom if your computer is infected with ransomware
- Be aware of current scams targeting individuals and businesses by following government sites such as SCAMWATCH
- Be suspicious of any unsolicited emails or text messages purporting to be from government agencies, banks, delivery services or other similar organisations – check the senders email address for clues and delete any suspicious email or look up the organisations main phone number and call if unsure
- Be suspicious of unsolicited phone callers purporting to be from Telstra, Microsoft, the Australian Taxation Office and do not provide any information, instead end the call – if unsure, look up their main number and call it to confirm
- Do not allow remote access to any computer or network resource by a third party unless it is arranged with Mansol

Portable Devices

- Smart phones and mobile computers must not be left unattended in public
- Smart phones and mobile computers must not be left in vehicles (locked or unlocked)
- Smart phones and mobile computers must not be stored in check-in baggage when flying
- Portable storage devices (e.g. USB drives, USB flash drives) should be vetted and checked for viruses prior to their use

Information Security Policy

- Portable storage devices require password protection if they are used to store any personal information (such as employee or participant information)

Social media

- Only those authorised to do so should represent the organisation on social media
- Personal information and confidential Brook RED information must not be posted or shared on social media
- When an employee leaves, their access to the organisations social media must be promptly removed

Printed material

- Personal information in printed format must be stored securely when not being used
- Personal information in printed format must not be left lying around
- When no longer required, printed material that contains personal information must be shredded or removed by a secure destruction service

Incidents

- A data breach or breach of privacy and confidentiality is an incident, follow the Incident process to manage and resolve the incident
- Incidents where individuals are at risk of harm as a result of the breach must be advised of the breach and assisted with ways to reduce their risk of harm from the breach
- Incidents where individuals are at serious risk of harm as a result of the breach are reportable to the Office of the Australian Information Commissioner

Definitions of Terms Used

Adware

Software that automatically displays or downloads advertising material such as banners or pop-ups

Backdoor

A technique to bypass a computer systems security undetected in order to access a computer or its data.

Bot

Self-propagating malware that infects its host and connects back to a central computer. Malicious bots can then be used to spy on user activity, steal passwords, relay spam, open backdoors, or perform attacks on other computers, websites or resources.

Data breach

An incident where personal and/or sensitive information has been accidentally or deliberately accessed and/or disclosed in an unauthorised fashion. Some common examples of data breaches include:

- Personal information accidentally mailed or emailed to the wrong recipients
- A locked filing cabinet containing personal files is broken into or left unlocked and accessed by unauthorised persons

Information Security Policy

- A computer or storage device used to store personal information is compromised as a result of a security breach, malware or poor security practices
- Personal information in printed form or on an insecure storage device is left in a public place
- Personal information accidentally or deliberately shared on social media

Malware
Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. Includes viruses, ransomware, spyware, adware and other

Patch
See “update”.

Phishing
Fraudulent emails purporting to be from reputable companies sent to fool users into revealing personal information such as passwords, bank account details or credit card numbers.

Ransomware
A type of malicious software designed to block access to a computer system until a sum of money is paid.

Spam
Also known as junk email, spam is unsolicited email usually to containing advertising, malware, or phishing.

Update
An update to a computer, tablet or smart phone operating system usually to correct security flaws (vulnerabilities) or correct errors.

Virus
A type of malicious software that install without the user knowing. A virus can replicate itself, modify computer programs, corrupt data, open backdoors or install adware, bots or ransomware.

Vulnerability
A flaw in a system that can leave it open to attack.

References
-

Information Security Policy

Document Control and Record of Changes

Version	Effective Date	Approved by	Summary of Change	Date of Next Review
Version 01	September 2019	Eschleigh Balzamo	Introduction of new policy	January 2020
Version 02	June 2021	Eschleigh Balzamo	Review and Update	June 2023

The General Manager has overall responsibility for this policy. If there are any questions regarding this policy, please direct these to the Business Services Manager or General Manager.