Information Security Policy and Guidelines

Scope
This policy applies to Brook RED Community Members, Nominated Support People, Board Members, employees, volunteers, and students on placement.

Purpose
To ensure that Brook RED has processes in place to secure personal and private information and to manage potential Information Technology (IT) *vulnerabilities*.

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

Policy
Brook RED outsources the management of its computer systems to external IT experts to maintain security and ensure general organisational efficiency.

Staff will inform management immediately if they become aware of an information security breach (such as *malware* and *ransomware*) and this will be considered and escalated to the external IT experts as appropriate.

A General Incident Report Form must be completed for serious breaches in accordance with the Responding to Incidents Policy and Procedure. For more information about collection and storage of personal and sensitive information, please refer to the Brook RED Privacy and Confidentiality Policy.

Procedure

General Security Precautions

- When sending group emails to Community Members or externally, use the 'Bcc' field rather than the 'To' field to ensure that the recipients cannot see other recipients email addresses
- Always password lock computers when they are unattended
- Operating system updates 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 enabled and must have a strong admin password
- Wi-Fi 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 to ensure that '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

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 sender's email address and delete any suspicious emails. Look up the organisation's main phone number and call if unsure
- Do not click on links from unknown senders
- 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 and 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 our IT experts

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
- 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'

Portable Devices

- Brook RED phones and laptops must not be left unattended in public
- Brook RED phones and laptops must not be left in vehicles (locked or unlocked)
- Portable storage devices such as USB drives should be checked for viruses prior to their use
- Portable storage devices require password protection if they are used to store any personal information (such as employee or Community Member 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

Information Security Policy

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

Data Breaches

Please refer to the Brook RED Privacy and Confidentiality Policy and Responding to Incidents Policy.

Definitions of Terms Used

Data Breach

A data breach is a type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen, or used by an unauthorised person or parties. A data breach where people are at risk of serious harm as a result is reportable to the Office of the Australian Information Commissioner.

Malware

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

Ransomware

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

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.

Vulnerabilities

Flaws in a system that can leave it open to attack.

Other Useful Definitions

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.

Information Security Policy

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.

Spam (or Junk Email)
Unsolicited emails usually to containing advertising, malware, or phishing.

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

References
Brook RED Privacy and Confidentiality Policy
Brook RED Responding to Incidents Policy and Procedure

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	July 2023
Version 03	August 2023	Eschleigh Balzamo	Review and Update	August 2024

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.