Digital Engagement Policy

Scope
This policy applies to Brook RED Community Members, Nominated Support People, Board Members, employees, volunteers, and students on placement. It is relevant to: telehealth and video conferencing platforms, telephones including messaging platforms, Brook RED's website, and Brook RED's social media.

Purpose
To ensure that Brook RED is safe, accessible, ethical, and consistent when engaging with Community Members, Nominated Support People, stakeholders, and the public across digital platforms.

Principles
Digital platforms and other technology are used at Brook RED to provide services to Community Members and to conduct business activities to support those services. Brook RED treats personal information with the utmost respect and care at all times and has specific provisions to ensure digital privacy and information security. This policy is in line with the National Safety and Quality Digital Mental Health Standards (NSQDMH), and should be used in conjunction with the Digital Engagement Guidelines.

Policy
This policy outlines the measures Brook RED takes to ensure that digital engagement with Community Members, Nominated Support People, stakeholders, and the public is transparent, secure, and accessible.

All Brook RED digital engagement must:

- Be in line with Brook RED's Digital Engagement Guidelines, Anti-Discrimination Policy, Personal Use of Communications Technology Policy, Privacy and Confidentiality Policy, Communication Policy and Style Guidelines, and Information Security Policy and Guidelines
- Be fit-for-purpose, and consider digital literacy and accessibility needs of the intended audience
- Uphold Brook RED's Guiding Principles, Code of Conduct and Employee Boundaries Policy
- Respect the privacy of Brook RED Community Members, Nominated Support People, Board Members, employees, volunteers, and students on placement
- Ensure that confidential and/or sensitive information owned by Brook RED is respected, and reasonable precautions are taken to ensure that information is not automatically collected by external platforms
- Use approved, secure communication channels
- Follow authentication and verification procedures
- Follow digital incident reporting procedures

Digital Engagement Policy

Data Privacy & Security

- Brook RED outsources the management of its computer systems to external IT experts to ensure systems meet Australian data security expectations and ensure general organisational efficiency
- Consent from the Community Member must be obtained prior to collecting, using, and storing a Community Member's information. Brook RED must provide reasons why the information is needed, and how and where the information is stored - refer to the Decision Making and Service Consent Policy and the Information Security Policy for further information
- Where collection of personal or sensitive information is required, Community Member digital information must be stored within our secure cloud server, which requires ID, password, and multi-factor authentication to access information
- Staff must complete a Digital Incident Report Form if they become aware of an information security breach, this will be considered and escalated to the external IT experts as appropriate
- Brook RED will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant employees (refer to the Information Security Policy)
- Brook RED phones and laptops:
    - Must not be left unattended in public
    - Must not be left in vehicles (locked or unlocked)
    - Should be transported with care if they contain Community Members information
- Brook RED will ensure that appropriate backup and recovery procedures are in place to prevent data loss
- At all times, all files stored on Community Members are made available to them. In the event that Brook RED winds up as a going concern, we will endeavour to contact all current or previous members and let them know that the organisation is closing and that a digital copy of their file will be made available to them upon request. The closing date and information will be available on the website and contact details will be updated on the website for data requests.
- All business-related files will be securely backed up and stored by the Business Services Manager.

Digital Incident Response

- Verbally notify Line Manager of all digital incidents
- Record incidents using a 'Digital Incident Report Form' and forward copies of forms to the Operations Manager and the General Manager within **two business days** of the incident occurring
- If necessary, external IT experts will be advised of the incident
- If necessary, the Office of the Australian Information Commissioner will be notified

Digital Business Continuity

To mitigate the impact of any digital service disruption (including outages):

Digital Engagement Policy

- Brook RED will ensure that staff are adequately trained to identify and respond to digital incidents, including following open disclosure guidelines
- Staff engaging in direct service provision will discuss alternative support options in the event of digital tool failure at the commencement of service engagement
- Reasonable efforts will be made to communicate digital outages to potentially affected parties

Digital Governance

Management will:

- Oversee the digital risk register and ensure that digital risk is discussed at the Board level
- Manage agreements and service level expectations with external IT experts to ensure compliance with the NSQDMH Standards
- Monitor subcontractor performance in relation to digital risk, security, accessibility, and system development
- Ensure digital policies and procedures, including digital and cybersecurity risk assessments and accessibility checks, are reviewed annually

In the event of a digital incident, Management will:

- Review any digital incidents received
- Ensure the appropriate parties have been contacted regarding the incident
- Respond to and/or escalate any digital incidents to the appropriate services and/or authorities where required
- Ensure open disclosure procedures are followed and recorded
- Log forms in the 'Incidents Register'
- Analyse all incidents every six months, analysis reports will be reported to the Board bi-annually
- Utilise information gathered and learnings from digital incidents to inform quality improvement measures.

Definitions of Terms Used

Digital Engagement

The use of digital platforms (such as websites, telephones, video conferencing) to interact with an intended audience.

Digital Incident

A digital incident is an event or series of events which may be related to hardware or software that compromises the confidentiality, integrity, or availability of information or a digital system. Examples of digital incidents include data breaches, platform outages, data loss, or cybersecurity incidents (eg, scam, phishing, malware).

References

Australian Open Disclosure Framework (ODF)
Australian Privacy Principles (APPs)
Brook RED Communications Policy
Brook RED Community Member and File Information Guidelines

Digital Engagement Policy

Brook RED Decision Making and Service Consent Policy
Brook RED Information Security Policy
Brook RED Privacy and Confidentiality Policy
Brook RED Responding to Incidents Policy and Procedure
Brook RED Vision, Mission, and Guiding Principles
National Safety and Quality Digital Mental Health Standards (NSQDMH)
Web Content Accessibility Guidelines 2.1

Document Control and Record of Changes

Version	Effective Date	Approved by	Summary of Change	Date of Next Review
Version 01	November 2025	Blake Barber	Introduction of new policy	September 2027

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.