Privacy Policy

Promote Inclusion, Show Empathy, Act with Integrity and Encourage Wellness

CONTENTS

1 PURPOSE

1.1 Bay & Basin Community Resources Limited/BCR Communities (BCR) understands that your privacy is important to you and we are committed to handling your personal and health information responsibly in compliance with the *Privacy Act*

1988 (Cth), the Australian Privacy Principles, *Health Records and Information Privacy Act 2002 (NSW)*, the Health Privacy Principles, the Aged Care Quality Standards, the NDIS Practice Standards and the National Principles for Child Safe Organisations.

1.2 The purpose of this Policy is to outline how BCR meets its obligations and how we handle the personal and sensitive information which:

1.2.1 our clients provide to us so we can provide them with supports and services and/or

1.2.2 candidates for positions applied for at BCR provide as part of their employment or engagement application.

2 SCOPE

2.1 This policy applies to all of BCR's operations.

3 INFORMATION WE COLLECT

3.1 The type of information we collect about you depends on the nature of your relationship with BCR whether, for example, you are a client, participant, job applicant, contractor, volunteer or staff member.

3.2 This information may include:

3.2.1 identifying and contact information such as name, date of birth, address, telephone number, email address,

3.2.2 government identifiers such as Medicare number, My Aged Care ID, Tax File number,

3.2.3 financial information, such as banking, payment and contribution details,

3.2.4 health information required to provide you with the supports and services you seek, and

3.2.5 information to deliver culturally appropriate services, such as religious, racial and ethnic background including if you identify as an Aboriginal and Torres Strait Islander person.

4 USE AND DISCLOSURE OF YOUR PERSONAL INFORMATION

4.1 BCR only collects personal information (including sensitive information) to:

4.1.1 provide you with supports and services (including third party products and services) you've applied for, to identify you, to manage your account and improve the services you receive,

4.1.2 consider your application for employment, volunteering or contracting services to confirm the information you've provided relating to experience, previous employment, and reference and compliance checks, and

4.1.3 comply with other relevant legislation and BCR policies and procedures.

4.2 By applying for or using any of the supports or services we provide and/or by providing us with your personal information, you agree to your personal information being collected, held, used and disclosed as set out in this Privacy Policy.

4.3 Whenever it is reasonable and practicable to do so, we will collect your personal information directly from you. If we are unable to collect information directly from you, we may also collect information from third parties to manage your supports and services and to better understand you, your preferences and interests.

4.4 We also use this information to comply with our legal obligations.

4.5 Some uses include:

4.5.1 identifying you,

4.5.2 providing and managing a product or service, including assisting you to complete online applications, answering your enquiries and complaints,

4.5.3 planning and delivering your supports and services,

4.5.4 helping us to improve the delivery of supports and services, enhance our relationship with you and to effectively manage risks,

4.5.5 enabling contact with a nominated person, General Practitioner or other health professionals involved in your care,

4.5.6 understanding your interests and preferences so we can tailor our products, services and marketing to tell you about other products and services that may be of interest to you,

4.5.7 managing our rights and obligations regarding external payment systems, including claiming and receiving funding due to us in advance or in arrears for services planned or provided to you,

4.5.8 assessing an application for employment, engagement or volunteering with us,

4.5.9 interacting with regulators and government departments or agencies in relation to a complaint made by you or your representative, or an incident that is reportable to a regulator under an Act or regulation, and

4.5.10 complying with legal or regulatory obligations imposed on us.

4.6 BCR may disclose your personal information to our workers and registered Third Party Providers when you consent to receive supports or services from them. We only disclose the personal information required to fulfil these services. All workers and registered Third Party Providers are vetted, verified and bound to respect the privacy of your personal information.

4.7 If you choose not to provide us with some or all of the information we request, we may not be able to provide you with the supports and services you require.

4.8 BCR will not send personal information about an individual outside Australia without:

4.8.1 obtaining the consent of the individual (in some cases this consent will be implied) or

4.8.2 otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

5 HOW WE USE YOUR INFORMATION TO TELL YOU ABOUT OUR SUPPORTS AND SERVICES

5.1 We may use your personal information to tell you about the supports or services you have requested or that we think might benefit you via:

5.1.1 email,

5.1.2 SMS, or other electronic notification,

5.1.3 social media and other digital platforms,

5.1.4 our website or software applications,

5.1.5 mail, or

5.1.6 telephone.

5.2 You can contact us at any time to 'opt out' of receiving these communications by calling us on 1300 222 748 or emailing us at info@BCRCommunities.com.

6 STORAGE AND SECURITY OF YOUR PERSONAL INFORMATION

6.1 BCR takes reasonable steps to ensure that the personal or health information it collects and holds is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

6.2 Personal and health information kept by BCR in printed form is stored in secure premises. In electronic form, it is held in secure storage systems requiring login details and passwords. Access to personal or health information is limited to those who specifically require it to conduct their responsibilities.

6.3 Our workers are bound by a Code of Conduct to maintain the confidentiality of your personal information. Third Party Providers are bound by a Brokerage Agreement to maintain the confidentiality of your personal information. All employees and volunteers of BCR Communities undertake privacy training so that they know how to keep your information safe and secure. Other parties are bound by Confidentiality clauses in our agreements with them.

7 ACCESSING AND CORRECTING PERSONAL INFORMATION WE HOLD ABOUT YOU

7.1 BCR takes reasonable steps to ensure that the information we hold about you is accurate, complete and up-to-date. To assist us with this, please provide us with correct information and inform us if your details change.

7.2 You have the right to access your personal information and request any corrections. Please contact us if you wish to view and/or correct personal or health information we hold about you. For security reasons, a written request may be required to access your health information. We are committed to granting you access to your personal information within a reasonable time frame. We will not refuse you access unless there are legal reasons for doing so. In such circumstances, we will explain those reasons to you.

7.3 If you have any questions about how we deal with personal information, wish to complain about a breach (or suspected breach) of your privacy, or correct your personal information, please contact us emailing info@BCRcommunities.com or calling 1300 222 748. BCR's Privacy Officer is BCR's Chief Executive Officer.

7.4 If the matter is not resolved to your satisfaction, you can contact:

Office of Australian Information Commission (OIAC),

GPO Box 5288,

Sydney NSW 2001

Phone: 1300 363 992.

Email: foi@oaic.gov.au

Website: www.oaic.gov.au

8 PROTECTING YOUR PERSONAL INFORMATION

8.1 BCR is committed to keeping secure the Personal and Sensitive information you provide to us. We will take all reasonable steps to ensure the information we hold is protected from misuse, interference, loss, from unauthorised access, modification or disclosure.

8.2 We hold your personal information in a combination of hard copy and in electronic form. Some of your information is in secure data centres that are located in Australia and some with selected service providers, including cloud service providers.

8.3 Our information technology systems ensure we can meet the needs of BCR, ensure the protection of consumer, worker and organisation information and support the collection of service delivery data and reporting obligations outlined in our Funding and Grant Agreements.

8.4 We hold your personal information for as long as it is required to provide you with supports or services, or for any period we are required to keep that information by law. If we no longer require your personal information for any purpose, we will

take reasonable steps to securely destroy or permanently de-identify that information in accordance with destruction and retention requirements.

8.5 BCR's workers shall NOT make any statement to the press, radio or television station or to any reporter for the media. If a BCR worker is approached to make a statement or comment, they are to refer the person to the BCR Chief Executive Officer.

9 CYBER SECURITY

9.1 Strategies adopted by BCR to ensure the safety of data include:

9.1.1 we only utilise data storage physically based in Australia (data sovereignty) and only accessible within BCR's private network,

9.1.2 utilising a Unified Threat Management firewall (UTM),

9.1.3 protecting all computers with passwords and only granting users access to data that they require to do their job,

9.1.4 restricting access of service delivery staff to the data of clients they are working with or likely to work with and to information directly related to their work such as the support plan and notes, and

9.1.5 utilising mobile device manager (MDM) software to manage all access to data by support workers and other staff using BCR mobile phones. This includes remote wipe and remote delete functions for use in the event of loss of the device.

10 ELIGIBLE DATA BREACH

10.1 Not all data breaches are required to be notified to the Information Commissioner and affected individuals. The new notification requirements relate only to an Eligible Data Breach (a concept as defined in the legislation). An Eligible Data Breach is a data breach involving personal information that is likely to result in Serious Harm to any individual who the information relates to.

Serious harm can include:

10.1.1 serious physical harm,

10.1.2 psychological harm,

10.1.3 emotional harm,

10.1.4 economic harm,

10.1.5 financial harm,

10.1.6 serious harm to reputation, and

10.1.7 other forms of serious harm that a reasonable person in the organisation's position would identify as a possible outcome of the data breach.

10.2 Although individuals may be distressed or otherwise upset that a data breach has occurred, this is not of itself sufficient to trigger the requirement to notify unless a reasonable person in the organisation's position would consider that the likely consequences for those individuals would constitute a form of Serious Harm.

11 WHAT HAPPENS IF THERE IS A DATA BREACH

11.1 In the event of any loss, or unauthorised access or disclosure of your personal information that is likely to result in serious harm to you, we will investigate and notify the Office of the Australian Information Commission (OAIC) and other relevant regulatory bodies, and notify you as required under Privacy Laws.

11.2 BCR's Data Breach Response Plan outlines the process to be implemented, including:

Step 1 - Contain the breach

11.3 Contain the breach, make a preliminary assessment and designate person/team to coordinate response. BCR's Chief Executive Officer and Executive Managers will be notified of the suspected data breach.

Step 2 - Assess and evaluate the risks for parties associated with the breach

11.4 Assess and evaluate the risks for individuals and BCR (the parties associated with the breach). Consider whether the data breach is an Eligible Data Breach and whether a breach notification is required. Establish the cause and extent of the breach and identify the risk of harm.

Step 3 - Consider breach notifications

11.5 If the breach or suspected breach may result in serious harm to an individual or BCR, BCR's Directors and relevant government bodies will be informed. It is important to note that not all breaches necessarily warrant notification.

Step 4 - Take action to prevent future breaches

11.6 Fully investigate the cause of the breach and consider developing and implementing a prevention plan. Make appropriate changes to policies, procedures and relevant software. Review and revise relevant staff training practices.

12 NOTIFYING THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSION (OAIC)

12.1 Once BCR Communities has reasonable grounds to believe an Eligible Data Breach has occurred, we will provide a statement to the OAIC as soon as practicable after we become aware of the eligible data breach.

12.2 We will advise the OAIC if we believe that another entity regulated by the Notifiable Data Breaches Act is involved in the eligible data breach.

13 COMPLIANCE WITH THIS POLICY

13.1 If there is reason to believe that a director, committee member or worker has failed to comply with this Policy, it will be investigated in accordance with relevant Policies and Procedures.

13.2 Failure of a director, committee member or worker to comply with this Policy may result in:

13.2.1 the director or committee member being asked to resign their position or

13.2.2 the worker facing disciplinary action and/or reasonable management instruction in accordance with the Performance Management and Disciplinary Policy and Performance Management and Disciplinary Procedure.

14 DEFINITIONS AND TERMS

14.1 **Client:** an individual to whom BCR provides a support or service.

14.2 **Client's carer(s):** a person/people, other than BCR workers, who provides unpaid care and support to a client and includes parents and guardians and other support people.

14.3 **Director:** an individual appointed to the Board of Directors responsible for contributing to the collective decision making of the Board.

14.4 **Executive Manager:** a member of BCR's Management Team.

14.5 **Personal information:** information about you that also identifies you.

14.6 **Third Party Provider:** a business that is not affiliated with BCR that provides services to BCR and/or clients while maintaining separation from BCR as a contracted entity.

14.7 **Sensitive information:** information about you such as health, disability, ethnic origin, beliefs or sexual orientation.

14.8 **Serious Harm:** harm that is "more probable than not" having regard to a number of factors listed in the Notifiable Data Breaches Act including (not an exhaustive list):

14.8.1 the kind of information;

14.8.2 the sensitivity of the information;

14.8.3 how the information is protected;

14.8.4 who the persons are who could have obtained the information; and

14.8.5 the nature of the harm.

14.9 **Support workers:** staff who provide direct supports and services to clients.

14.10 **We, us, our:** BCR.

14.11 **Workers:** BCR's staff, volunteers and contractors.

14.12 **You, your:** BCR's clients and workers.

15 RELATED LEGISLATION AND DOCUMENTS

Aged Care Quality Standards

Australian Privacy Principles

Data Breach Incident Report Form

Data Breach Matrix

Data Breach Response Plan

Health Privacy Principles

Health Records and Information Privacy Act 2002 (NSW)

National Principles for Child Safe Organisations

NDIS Practice Standards

Privacy Act 1988 (Cth)

16 FEEDBACK

16.1 Workers and clients can provide feedback about this document by emailing info@BCRCommunities.com.

17 APPENDICES

17.1 Data Breach Incident Report Form

17.2 Data Breach Matrix

17.3 Data Breach Response Plan

18 DOCUMENT VERSION CONTROL

18.1 BCR will maintain a high standard of quality and control of all documented information and records. All documents (either retained or referred to) will be current, suitable for use, accessible, quality controlled, and stored in a safe and secure location.

18.2 BCR policies and procedures will be reviewed by the relevant responsible officer either:

18.2.1 prior to the mandatory three year review period or

18.2.2 when an incident or a known change (legislative or internal) has occurred or a complaint or feedback has been received that relate to specific BCR policies and/or procedures,

whichever occurs first.

Section 1				
	Title	Privacy Policy		
	Policy Location	Intranet		
	Responsible Officer	Chief Executive Officer		
	Created By		**Date Created**	16/08/2023
	Date Approved	16/08/2023	**Board to Approve all Modifications**	No
	Reviewer	Executive Team		

Section 2	**Version No**	**Modified/Reviewed By**	**Modifications Made**	**Date**	**Status**
	001		Policy approved and implemented	16/08/2023	Approved
	002		Reformatted original document	20/11/2023	Draft
	003	Executive Team	Added definition for Director and Executive Mgr	05/02/2024	Draft
	004	Executive Team	Removed reference to information directly related to employment	18/03/2024	Approved

APPENDIX 1 - DATA BREACH INCIDENT REPORT FORM

APPENDIX 1

DATA BREACH INCIDENT REPORT FORM

Details of person reporting the incident			
Full name		Title	
Contact number			
How did you find out about the data breach			
Name of person who notified you			
☐ Male ☐ Female ☐ Staff ☐ Visitor ☐ Contractor ☐ Volunteer ☐ Client ☐ Other……			
Date of breach		Time of breach	am/pm
Date you were notified		Time you were notified	am/pm
Location of data breach			
STEP 1 – CONTAIN **Initial details of data breach**			
Details of data which has been accessed			
Details of the extent of the data breach			
Details of any persons immediately notified of data breach			
Date persons notified		Time persons notified	am/pm
Did the person who notified you of the breach give any other relevant information about the breach?			
Describe immediate action taken to contain the breach (if any)			
You must notify the Chief Executive Officer (CEO) of the data breach			
Date CEO notified		Time CEO notified	am/pm

DATA BREACH INCIDENT REPORT FORM

PART 2 – TO BE COMPLETED BY MANAGER RESPONSIBLE FOR ASSESSING AND RESPONDING TO THE DATA BREACH	
Full name	**Title**
Contact number	
STEP 2 – ASSESS and EVALUATE *(Refer to Data Breach Response Plan)*	
What information does the breach involve?	
What was the cause of the breach?	
What is the extent of the breach?	
What damage or harm has been or could be caused by the breach?	
How can the breach be contained, if it has not been already?	
Risk associated with the type of personal information involved	
Who is affected by the breach?	
Does the type of personal information that has been compromised create a greater risk of harm?	
The context of the affected information and the breach	
What is the context of the personal information involved?	
What parties have gained unauthorised access to the affected information?	
Have there been other breaches that could have a cumulative effect?	
How could the personal information be used?	
The cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	
Is there evidence of theft?	
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	
What was the source of the breach?	
Has the personal information been recovered?	
What steps have already been taken to mitigate the harm?	

DATA BREACH INCIDENT REPORT FORM

Is this a systematic problem or an isolated incident?	
How many individuals are affected by the breach?	
The risk of serious harm to the affected individuals	
Who is the recipient of the information?	
What harm to individuals could result from the breach?	
Do you consider the data breach is an *eligible data breach* (refer to Privacy Policy and Data breach response plan)	Yes ❑ No ❑ If yes, the affected parties must be notified
STEP 3: NOTIFY **Notification to affected individuals must include**	
A description of the breach/incident	Yes ❑ No ❑
Type of personal information involved	Yes ❑ No ❑
An account of the organisation's response to the breach	Yes ❑ No ❑
Assistance offered to affected parties	Yes ❑ No ❑
Other information sources designed to assist in protecting against identity theft or interferences with privacy, such as www.oaic.gov.au;	Yes ❑ No ❑
The organisations contact details	Yes ❑ No ❑
Whether a regulator or other external contact has been notified of the breach	Yes ❑ No ❑
The legal implications	Yes ❑ No ❑
Information on how people or organisations can lodge a complaint with the organisation	Yes ❑ No ❑
Information on how people or organisations can lodge a complaint with the OAIC	Yes ❑ No ❑
Information on how people or organisations can lodge a complaint with the relevant state or territory privacy or information regulator	Yes ❑ No ❑
NOTIFICATION TO THIRD PARTIES ***The CEO must determine whether it is necessary to notify any of the following***	
Office of the Australian Information Commissioner	Yes ❑ No ❑ Date actioned ……
Police	Yes ❑ No ❑ Date actioned ……
Insurance Provider	Yes ❑ No ❑ Date actioned ……
Credit card companies and financial institutions	Yes ❑ No ❑ Date actioned ……
Professional or other regulatory bodies	Yes ❑ No ❑ Date actioned ……

DATA BREACH INCIDENT REPORT FORM

Other internal or external parties who have not already been notified	Yes ❑ No ❑ Date actioned ……
Agencies that have a direct relationship with the information, the subject of the breach	Yes ❑ No ❑ Date actioned ……
Other risks ***Detail whether there are any broader implications of the data breach to the organisation***	
Loss of public faith and trust in the organisation? Yes ❑ No ❑ *If Yes, please provide details*	
Damage to reputation? Yes ❑ No ❑ *If Yes, please provide details*	
Liability? Yes ❑ No ❑ *If Yes, please provide details*	
Breach of any other privacy provisions? Yes ❑ No ❑ *If Yes, please provide details*	
If the CEO determines that it is not necessary to notify affected individuals, the OAIC or third parties of an eligible data breach, the decision (including reasons and any relevant exception) must be recorded here and must be sign off by the CEO	
Detail of reasons for decision not to notify	

CEO sign off on decision not to notify			
Name		**Signature**	
Date:		**Time:**	

DATA BREACH INCIDENT REPORT FORM

STEP 4 - REVIEW
Fully investigate the cause of the breach and consider developing a prevention plan. Consider whether there are any changes which can be made within the organisation which will help prevent future data breaches, including policies, procedures and staff training. .
Identify what communication needs to be initiated to rebuild confidence and business reputation.
Name of person completing this report (print): ..... Signature ..... Date.....Time .....

APPENDIX 2 - DATA BREACH MATRIX

APPENDIX 2

DATA BREACH MATRIX

This Data breach matrix should be used as part of the process of assessing and evaluating a data breach as outlined in the Data Breach Response Plan

DATA BREACH MATRIX					
Type of impact	**Lowest ← Severity → Highest**				
	Minor = 1	**Low = 2**	**Moderate = 3**	**Major = 4**	**Extreme = 5**
The nature and type of information the breach involves [*sensitive information refers to information which is of a commercial, personal or proprietary nature and which may, if disclosed, impact upon individuals or organisations*]	No sensitive information pertaining to individuals or organisations exposed	Sensitive information exposed in respect of individuals or organisations which has the potential to cause only minor distress to the parties	Sensitive information exposed in respect of individuals or organisations which has the potential to cause substantial short term distress to the parties	Sensitive information exposed in respect of individuals and organisations which has the potential to cause substantial short to long term distress to the parties	Sensitive information exposed in respect of individuals and/or organisations which has the potential to cause significant long term distress to multiple parties, broad public concern, media coverage, Parliamentary inquiry or Royal Commission
The cause of the breach	No risk of ongoing or repeat breaches	Negligible risk of ongoing or repeat breaches and steps taken to mitigate any future risk	Moderate risk of ongoing breaches and further exposure of information, source of breach identified and steps being taken to mitigate	High risk of ongoing breaches and further exposure of information, source of breach not confirmed and steps being taken to mitigate	High risk of ongoing breaches and exposure of further information, evidence of theft, information not adequately anonymised and source of breach unknown
The extent of the breach	Little to no risk of serious harm to an individual or organisation	Risk of serious harm to a single individual or a small group of identifiable individuals	Risk of serious harm to multiple individuals or an organisation	Risk of serious harm to multiple individuals and organisations	Risk of serious harm to entire database of individuals, organisations and others
The damage or harm that has been or could be caused by the breach	No damage or harm caused. No future damage or harm forecasted	Minor and localised damage or harm has been or could be caused by the breach	Significant short term damage or harm has been or could be caused by the breach	Significant long term damage or harm has been or could be caused by the breach	Significant and widespread short and long term damage or harm has been or could be caused by the breach

APPENDIX 2

DATA BREACH MATRIX

Difficulty of containing the breach	Breach contained	Little to no risk that the breach will not be contained	Work underway to contain the breach. Moderate to low risk that breach will not be contained in the short term	The breach will not be contained in the short term and work is underway to contain the breach	Significant difficulty in containing the breach. Likelihood of breach being contained in the short to medium term, slim.
Risk of loss of public faith and trust in the organisation	No risk of loss of public faith and trust in the organisation	Minimal impact to public faith and trust in the organisation	Moderate impact to public faith and trust in the organisation over the short term	Significant impact to public faith and trust in the organisation over the short to medium term	Significant long term impact to public faith and trust in the organisation. Potential or actual consequences for organisations activities
Damage to reputation of organisation	No risk to the reputation of the organisation	Minimal impact on the reputation of the organisation	Moderate short-term impact to the reputation of the organisation	Significant impact to the reputation of the organisation over the short to medium term	Significant long term impact to the reputation of the organisation. Potential or actual consequences for organisations activities
Economic and commercial impact of the breach on the organisation	No economic or commercial impact on the organisation	Minimal economic or commercial impact on the organisation	Moderate short-term economic and commercial impact on the organisation	Significant economic and commercial impact on the organisation over the short to medium ter	Significant short and long term economic and commercial impact on the organisation
Potential for civil or criminal liability resulting from the breach	No risk of civil or criminal liability	Minimal risk of civil or criminal liability	Moderate risk of civil or criminal liability	Significant of civil or criminal liability	Very high risk of civil or criminal liability
Has the incident breached any other privacy provisions or relevant laws	No breach of any other privacy provisions or laws	Breach of other privacy provisions or laws – minimal impact	Breach of other privacy provisions or laws – moderate impact	Breach of other privacy provisions or laws – significant impact	Breach of other privacy provisions or laws – very high impact

DATA BREACH MATRIX

Summary of Risks		

Record of Decision		
Has a notifiable breach occurred	Yes ❑	No ❑
Are there affected individuals they need to be notified	Yes ❑	No ❑
Does a statement need to be submitted to OAIC	Yes ❑	No ❑

CEO sign off
Name of CEO
Signature
Date

APPENDIX 3 - DATA BREACH RESPONSE PLAN