HUMAN RESOURCES POLICY

HR03 Privacy, Dignity, Confidentiality and Data Integrity

This is about how Bedford will treat everyone with respect, keep things about them private and report certain privacy problems to the Government.

1. PURPOSE

To ensure that an individual's right to be treated with respect and dignity and to have personal information managed in an open, safe and transparent way is upheld.

To ensure that personal information/data that Bedford collects, uses, stores or holds is maintained in line with data integrity and privacy principles and that any data breach is identified, investigated, managed and reported in line with same.

2. SCOPE

This Policy applies to all Bedford operations and divisions as well as all Bedford data management systems, including our internet website.

3. DEFINITIONS

CIMS – Bedford's Customer Information Management System.

Client – Any person receiving funded services from Bedford, including persons with a National Disability Insurance Scheme (NDIS) Plan (also called NDIS Participants).

Data – Information on a person or business obtained through marketing, telesales, fundraising, application/recruitment, client management processes, email/intranet or via the Bedford website that is kept either on our internal information systems or in a cloud environment.

Bedford maintains the following types of data:

- Data that is personally identifiable – Data that has the capacity to identify a person. This can include name, dates of birth, addresses/contact details, medical or support information, bank account or credit card details, tax file number, Centrelink/Medicare numbers and so on.
- Company information – This is data that is used by Bedford to manage its operations and includes such things as processes, policies, contracts, invoicing systems and so on that do not contain personal information.
- Publicly available information – Information that is part of the public domain, including on websites, marketing material, publicly used forms etc.

Data Breach – See Privacy/Data breach below.

Eligible Data Breach – Only data breaches which can be categorised as an 'eligible data breach' require notification in line with this Policy. An eligible data breach arises when either:

- There is unauthorised access or disclosure of personal information and a reasonable person would conclude that the disclosure or access is *likely to result in serious harm* to those individuals affected; or
- Information is lost in circumstances where unauthorised access or disclosure is likely to occur and assuming that unauthorised access or disclosure were to occur, a reasonable person would conclude that the disclosure or access is *likely to result in serious harm* to the affected individuals.

Employee – A person with a disability receiving supported employment at Bedford.

Member – A person with a disability engaged in Bedford Day Options service.

Personal Information – Any kind of data or information that can be considered to identify an individual.

Privacy Breach/Data Breach – A privacy or data breach can include:

- Passing on private information to another person without appropriate authorisation.
- Loss or misplacement of a file or written information containing personal or personally identifiable information, including via email, USB flash drive, portable hard drives, laptops and so on.
- Inappropriate or unauthorised use or access of a person's private information.
- Loss or theft of passwords or other confidential access data.
- Cyber activity such as hacking of information or unauthorised computer access.

Resident/Tenant – A person with a disability who resides and receives funded services at Balyana, in a Bedford supported community property or in Bedford Housing Victoria.

Serious Harm – Relates to the likelihood that a data breach may cause an individual to whom the information relates serious harm with consideration to the information's sensitivity, the types of people who have obtained the information, the likelihood of the information being used to harm a person, if the information is protected by security, whether these measures can be circumvented and the nature of the harm likely to be caused.

Staff – Any persons engaged by Bedford to provide funded services or support the provision of such services. This can include volunteers, mainstream students, contractors and labour hire workers.

4. POLICY

Bedford is bound to act in accordance to the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988, the Privacy Amendment (Notifiable Data Breaches) Act 2017 and the 13 Australian Privacy Principles that govern how organisations should handle information. Equally, it is also required to comply with the European Union General Data Protection Regulations (2018).

Bedford will maintain and uphold the privacy of individuals in line with the above legislation, the NDIS QA and Safeguarding Rules, its' duty of care responsibilities and the rights of individuals to be treated with dignity and respect at all times.

Privacy or data breaches will be promptly investigated and reported in line with legislative and Corporate requirements

Bedford staff must comply with this Policy and must act to protect the confidentiality and privacy of any individual that it collects information about. Failure to do so may result in disciplinary action.

4.1. Personal Information Collected

Bedford collects a variety of personal information, including full name, date of birth, address, career and educational history, occupation, references, medical reports/ history, allied health professional reports, bank details, Tax File Numbers, Centrelink details, Email addresses and credit card details.

As part of its Lotteries activities, Bedford also has contracts with external agencies to conduct lotteries on their behalf. This includes the gathering, maintaining and storage of customer and third-party business information on our internal data systems.

4.2. Collection/Source of Information

Personal information will be obtained only where it is relevant and necessary to:

- Fulfil legal and contractual obligations.
- Protect the health and/or safety of the individual or others.
- Provide appropriate training and support services.
- Maintain business operations (billing, marketing and so on).
- Assess suitability for a role/position.

Information will be sourced directly from the individual, whenever possible. However, if additional information is required from another party, Bedford will take reasonable steps to ensure the individual understands why such information is required and obtains their permission on an Information Release Authority Form. Each Information Release is to have a timeframe for currency.

4.3. Disclosure of Information

All information collected is for the sole use of Bedford and will not be disclosed (verbally or in writing) to any third party without the expressed permission of the individual.

It is the right of the individual to refuse to give consent for the release of information. This request will be respected when it is exercised; and the implications of this will be discussed with the individual.

Prior to disclosing any information, Bedford will obtain their permission on a Bedford Information Release Authority form. Each Information Release is to have a timeframe for currency.

Such data will not be disclosed to any overseas recipients.

4.4. Exceptions to Disclosure

The following exceptions apply with respect to obtaining written authority to release information:

- Where disclosure is required or authorised by any law or when there is an over-riding public interest or professional responsibility.
- Where the information or file is the subject of a subpoena or is to be disclosed before a court or tribunal duly constituted in law.
- Where another staff member needs the information to provide training/support for the individual, or who may need to make decisions regarding the situation.
- Where releasing the information is necessary to avert, minimise or eliminate a serious and immediate danger to the health of a person or others. If the situation is 'serious' only, permission must be requested from the individual concerned. If permission is denied, no information can be released until there is 'immediate danger'.

- When it is believed that a person or group of people are at risk of harm from others or as a result of their own actions, and adverse outcomes might reasonably be expected unless appropriate services are provided (refer Bedford Policy Information Sharing Guidelines – Appendix).
- Where the information is required under Commonwealth Acts for the purposes of establishing a person's entitlements to Commonwealth benefits.
- Insurance Liability Cover requires that matters which give rise to, or may give rise to a claim, must be notified to the insurer. This also means that the insurers would require access to relevant information if an action is brought against Bedford Phoenix by an aggrieved service user.
- Due to Bedford's Duty of Care responsibilities, the CEO, Executive and relevant General Manager are to be advised of any allegations of impending or actual situations involving breaches of the law, Court appearances or bail conditions.
- Government (State and Federal) contractual requirements require certain information to be provided to the Government e.g. census, data collection exercises etc. Bedford will comply with relevant Government guidelines, including required privacy/confidentiality protocols and ensure that privacy is maintained.

4.5. Storage of Information

All reasonable steps to protect the security of personal information will be undertaken, this includes appropriate measures to protect and back-up electronic material and material stored and generated in hard copy.

Bedford Lotteries operations will use an accredited third-party e-security agency to store sensitive credit card information belonging to customers.

4.6. Access/Maintaining Quality of Personal Information

All requests for access are to be directed to Human Resources and will be treated seriously and reasonable steps will be taken to provide access within 30 days of the request. Refer to Australian Privacy Principles 12.3 for "exemptions to access" and 12.9 for "refusal to give access".

Bedford will provide access by allowing individuals to inspect, take notes of or ask for a copy of any personal information (as outlined in 4.1) that is held.

Requests for copies on information held on file are to be directed to the General Manager Human Resources and are subject to appropriate Information Release Authority. Bedford may impose charges for providing copies.

Bedford will take all reasonable steps to ensure that personal information that it collects and holds is accurate, up to date and complete. Everyone will be reminded to advise Human Resources at the earliest opportunity of any changes to their personal information so that records can be updated.

Such information can be updated/corrected at the request of an individual.

Information that is out of date will be removed from files and confidentiality destroyed.

4.7. Access by Auditors

Files can be reviewed by an authorised Government staff for the purpose of service provision audits.

Documents contained in a file that relate to regulatory quality compliance audits can be viewed by an authorised Third-Party auditor, providing that individual has given documented consent and a Bedford Privacy Officer has ensured that a designated delegate oversees this process.

Documents on client files may be viewed by approved Bedford staff for the purposes of an internal audit; access to highly confidential documents is to be approved prior and overseen by Human Resources or the relevant General Manager.

4.8. Access to Files

The Chief Executive Officer has access to all files/computer records and may delegate access to a record for a specific issue, otherwise access to files/computer records is restricted.

Access to files/computer records is limited to those that provide support and/or management of that individual.

Those individuals who receive several Bedford services e.g. supported employment, residential, social and community participation, information that is pertinent to an individual's welfare and health status/needs will be communicated between service staff in each area. Records of support provided in any of the services is available in CIMS to all the staff that provide support to that individual.

Participants, employees, residents and members may request and gain access to their personal information and will be able to view all information in the presence of Bedford staff. However, certain information may not be disclosed such as psychological or other reports written by a Third Party.

Individuals may request to gain access to their Return to Work file; such requests must be made in accordance with the Return to Work SA Act, Workplace Injury Rehabilitation and Compensation Act (Vic) and WorkCover NSW Act.

Access to Fundraising and Finance data is limited to authorised staff only with access dependant on role and level of authority.

4.9. Photographs/Media

Bedford will obtain written permission via a Media Consent Form for any display, publication or release of any photograph or visual image/file including on social media.

Social and Community Participation/Day Options services utilise member photos in daily service activities (Activity plans, Mood Boards and so on). Consent for this is obtained via the Social and Community Participation/Day Options Photo Consent Form which is completed at Induction and annually during Individual Program review.

Should any of these photographs be required for use in media or public relations activities (as above), a separate Media Consent form must be completed.

4.10. Contact with NDIS Participants Families/Registered Plan Managers/Plan Nominees/Support Coordinator

A Service Agreement between Bedford (Provider of NDIS supports) and a Participant is written when an NDIS Plan is active or has been updated.

When the Participant chooses to have their representative sign this Agreement; any information about the supports being delivered by Bedford, their goals, aspirations can be openly exchanged/communicated between the representative and support staff, without the need to obtain further consent.

Additionally, if the Participant has appointed a Registered Plan Manager, Support Coordinator or Plan Nominee; the Participant upon signing the Service Agreement gives Bedford staff consent to liaise with such organisations/individuals regarding the payment of supports provided, applications for credit and any follow up of payments.

4.11. Transporting of Files

If a file is being transferred between sites, it can be transferred via 'safe-hand' in a sealed double envelope and stamped "confidential". If this is not possible, then the file is to be sent via Registered Mail in a sealed double envelope and stamped confidential.

When transporting a file or confidential documents via a vehicle, they must be secured out of sight and the vehicle must be locked when not occupied.

4.12. Data Security – Information Technology/Personal Computers/Offices

Electronic records will be protected from misuse, loss and unauthorised access; Management of Bedford Information Systems will:

- Apply a screen saver to all computers, which will activate within ten (10) minutes of inactivity.
- Ensure that access to any data base records is in line with policy and legislation.

Staff must immediately collect work from a printer and check their offices e.g. whiteboards, pin boards, desks etc to ensure that identifying or confidential information is not displayed.

Files and personal records must be stored in locked cabinets/drawers when not in use. They must not be left on desks in unlocked offices.

Fundraising and Lotteries operations will use an accredited third-party e-security system for storage, transfer and maintenance of customer/client data.

4.13. Disposal of Files and Information Technology Equipment

All files are kept for at least seven (7) years at which time they can be confidentially destroyed as directed by the General Manager Human Resources.

The General Manager ICT is responsible for ensuring that any hard drives relating to personal computers, printers and copiers have been erased before decommissioning.

4.14. Privacy Officers

The Chief Executive Officer will appoint Privacy Officers, who will be responsible for:

- Ensuring and monitoring compliance with this Policy.
- Having available a copy of the Privacy Act.
- Assisting with the resolution of any complaints or incidents regarding breaches in privacy.
- Referring issues and eligible/reportable data breaches to the Privacy Commissioner where appropriate and in line with Policy.

4.15. Privacy Complaints

A privacy complaint relates to any concerns/grievances that an individual may have with Bedford's privacy practices as it relates to personal information. This could include how information is collected, stored, used, disclosed or accessed.

Any individual that has provided Bedford with personal information has the right to make a complaint and have it investigated.

All complaints will be treated seriously, investigated fully and promptly and in a confidential manner.

Privacy complaints will be handled by the designated Privacy Officer, Executive or relevant delegate in line with Policy on Grievances/Problems and Complaints and relevant legislation.

4.16. Dignity

The dignity of all individuals will be respected and upheld by:

- Treating everyone with respect.
- Not obtaining, nor seeking to obtain, personal information that is not relevant to provision of quality training and support.
- Responding promptly and sensitively to situations where personal care or physical assistance is required or where the persons' privacy or dignity is at risk.
- Respecting the need to have interpreters.
- Being sensitive to cultural, ethnic and religious practices/customs.

4.17. Privacy Breach

Staff must immediately report any suspected or actual privacy breaches to Management.

Suspected Breaches/Investigation

If Bedford becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach, Management must immediately notify a Privacy Officer and Executive; who will then oversee an investigation to determine whether the breach is an "eligible data breach".

This must be completed within thirty (30) days of Bedford becoming aware of the potential breach. The aim of the investigation is to:

- Identify whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity;
- Identify the cause of the breach so that appropriate preventative and remedial action can be taken.

Notification – Eligible Data Breach

If a Bedford becomes aware that there are reasonable grounds to suspect that there has been an eligible data breach (whether following an investigation or without an investigation), then the Privacy Officer(s) must prepare a statement for the Privacy Commissioner that includes:

- Bedford's identity and contact details;
- A description of the eligible data breach;
- The types of information concerned; and
- Recommendations about the steps that individuals should take to protect themselves or mitigate harm.

Individuals affected by the eligible data breach must also be notified. Steps must be taken to notify affected individuals directly, for example, by calling them on the phone. If direct notification is unreasonably difficult or may cause further harm, then indirect notification, such as a notice on a website, may be used.

Notification Exemptions

In line with the Privacy Amendment (Notifiable Data Breaches) Act 2017; if Bedford is able to instigate remedial action following an eligible data breach, or potential breach sufficient to result in a reasonable person concluding that the unauthorised access, disclosure or loss is not likely to result in serious harm, then the eligible data breach is taken never to have been an eligible data breach. Reporting is then not required.

The determination of whether this applies is to be made by Executive and must be documented in the Privacy Incident Report

4.18 Recording Privacy Incidents

All activities in relation to a breach or a suspected breach must be recorded in the Issues Register in Skytrust as a Privacy Breach Incident.

4.19 Knowledge and Understanding of Procedures

During induction, all staff and service users will receive information regarding this Policy, including the possible consequences of breaching these requirements.

Feedback from employees on how well Bedford respects and protects their rights to privacy and confidentiality is sought via feedback surveys.

5. RESPONSIBILITIES

The responsibilities of various staff are detailed throughout this Policy, but in summary:

- **Executive** – Appoint Privacy Officers, ensure compliance with this Policy.
- **HR** – Provide staff induction on this Policy and related procedures.
- **Privacy Officers** – Monitor/ensure compliance with this Policy and assist with the investigation and resolution of any complaints.
- **General Manager ICT** – Security of electronic records; decommissioning of hard drives, monitor and approve access to systems, develop and promulgate procedures and processes to maintain information systems privacy and security, investigate and report on breaches/suspected breaches.
- **Managers** – Ensure that systems and processes are in place to protect and maintain privacy, reporting and investigating breaches/suspected breaches.
- **Staff** – Comply with this Policy, reporting breaches/suspected breaches.

6. ASSOCIATED DOCUMENTS

Bedford Policies and Procedures, including those relating to Induction, Information Sharing Guidelines – Appendix, Duty of Care, Data Access and Breaches, Information & Computer Systems, Information Release Authority Form, Media Consent Form, Bedford Information Sharing Form.

7. REFERENCES

Freedom of Information Act

National Standards for Disability Services (Rights) Privacy Act (1988)

Privacy Amendment Act (2000)

Privacy Amendment (Enhancing Privacy Protection) Act, 2012

Privacy Amendment (Notifiable Data Breaches) Act 2017

General Data Protection Policy of the European Union (2018)

13 Australian Privacy Principles

Australian Service Excellence Standards Disability Services Act, 1993

Return to Work SA Act 2015

WorkCover NSW 2015

Ombudsman SA - Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG)

DCSI Safeguarding People with Disability – Overarching Policy

National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018

HR04.01 FEEDBACK FORM

Bedford is committed to providing high quality services and meeting your needs.

We value your feedback – including complaints.

You can get help from a Contact Officer or Support Person to help you fill in this form and support you at any time while your feedback is being looked at.

This form needs to go to Human Resources; if you are lodging a complaint they will look at the best way to look at how things could be made better.

Your feedback is? (Please indicate your response with an X)

	Compliment - letting Bedford know what we do well and you have been happy about 
	General feedback - giving Bedford some ideas on how to improve our services 
	Complaint - letting us know that our services have not met your needs 

Do you want to remain anonymous (unidentified) and not provide your name and contact details?

No	Please complete your details on the next page.
Yes	Please note that if you choose to be unidentified, this may have an impact on how your feedback is managed because Bedford Management will not be able to obtain more details and will not be able to let you know what actions were taken.

Section 1: Personal details

First Name:	
Last Name:	
Postal address:	
Telephone Number:	
Mobile Number:	
Email Address:	

Do you require an interpreter?

Yes		**No**		**If Yes, Which Language?**	

Are you providing feedback on another person's behalf?

No *(Go to Section 3)*		**Yes**	***(Continue to Section 2)***

Section 2: Feedback made on another person's behalf

Please provide the following details about the Bedford client on whose behalf you are completing this for on or are acting on their behalf:

First Name:	
Last Name:	
Postal address:	
Telephone number:	
Mobile number:	
Email address:	

Please provide details of your relationship to the person on whose behalf you are acting: (Indicate your response with an X)

Legal Guardian:	
Advocacy Agency:	
Family Member:	
Friend:	
Other:	

Are we able to speak with the Bedford client who received the service? (Indicate your response with an X)

Yes		**No**	

If No, please provide the reason why:

Section 3: Please indicate with a X which of Bedford's services that the feedback concerns

	Supported Employment
	Community Access/Day Options
	Accommodation
	RTO (Training)

Section 4: Tell us about what is concerning you:

What action would you like taken or outcome are you seeking as a result of providing your feedback?

Section 5: Declaration

By signing this form you are saying that all the information you have given here is truthful and accurate to the best of your knowledge.

Signature:		**Date:**	

Thank you for taking the time to provide feedback about our service.