

HUMAN RESOURCES POLICY



HR03 Privacy, Dignity, Confidentiality and Data Integrity

Keeping things private

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 or sensitive information managed in an open, safe and transparent way is upheld.

To ensure that personal or sensitive 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.

This Policy is to be read in conjunction with HR Procedure; Privacy, Dignity, Confidentiality and Data Integrity

3. 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, up to and including termination of employment or placement.

4 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.

4. DEFINITIONS

ACIC - Australian Criminal Intelligence Commission – nationally accredited

ACIC Authorised User – a Human Resources staff member, who has been authorised to operate the ACIC nationally accredited criminal history check service.

Biometrics - A biometric is a measure of some physical or behavioural attribute of a person, which is intended to be unique, or sufficiently distinctive to assist in recognising who the person is. This includes photographs (e.g. in drivers' licences and passports), finger prints and so on. Bedford requires the provision of photographic evidence (drivers' license/passport) as part of the identity verification process during an application for a National Police Check

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/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 etc.
- 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.

Demographic Information - statistical data relating to the population and particular groups within a community, including a person's age, date of birth, gender, postcode, country of birth, indigenous status, occupation, disability status, language spoken or religious affiliation. Bedford uses certain demographic information, such as date of birth and address as part of the identity verification process during an application for a National Police Check

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.

National Police Check; a record of offender status/criminal history in Australia

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 – A person with a disability who resides and receives funded services at Balyana, or in Bedford Housing Victoria.

Sensitive Information - Sensitive information is a type of personal information and includes information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes (for instance as part of the verification process during an application for a National Police Check)
- biometric templates.

Serious Harm – 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.

5 ASSOCIATED DOCUMENTS

Bedford Policies and Procedures, including Procedure - Privacy, dignity, Confidentiality & Data Integrity, 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.

6 REFERENCES

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

ACIC – NPCS Accredited Body Agreement

ACIC – National Police Checking Service Handbook (Version 1, 2017)

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 Privacy Principles - Guidelines

Australian Service Excellence Standards Disability Services Act, 1993

Victorian Protective Data Security Standards, March 2018

Return to Work SA Act 2015

WorkCover Act NSW 2015

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

DHS SA Safeguarding People with Disability – Overarching Policy