

POLICY

TITLE:	Accounting Privacy Policy		
DIVISON:	COUNCIL		
ADOPTED BY:	COUNCIL		
DATE OF ADOPTION:	MAY 2023	DATE OF REVIEW:	MAY 2028
MOTION NUMBER:			
POLICY NUMBER:	CP47 v2.		
LEGISLATIVE REF:	Privacy Act 1988 (Cth) Information Act 2002 Section 206(3)(4) and Schedule 1 of the <i>Local Government Act 2019</i>		

THIS POLICY APPLIES TO: Council Members, Staff, Committee Members and Local Authority Members

1.0 SUMMARY

1.1 Purpose

To establish a framework pertaining to the privacy and confidentiality obligations of Council, including protecting all council members, staff, committee members and Local Authority Members from undue intrusion into their private information contained within council

1.2 Scope

This policy shall apply to all employees and elected members of Council and its Committees. This process will be reviewed every two years.

1.3 Policy Objectives

The objectives of this policy are:

- To ensure adequate controls are in place to minimise risk
- To promote transparency and accountability
- Uphold the reputation of the Barkly Regional Council
- Instil confidence in Council by community stakeholders and business partners
- Protect members and staff private information contained within council

1.4 Definitions

Privacy is mandated under the Privacy Act 1988 (Cth) ('the Act') to protect the privacy of individuals through the handling of their personal information, irrespective if the information is publically available. Under the Act, "personal information" is defined as information or an opinion, about an identified person or reasonably identifiable individual, regardless whether the information or opinion is true or not, and whether recorded in a material format or not.

Confidentiality is not mandated and is governed under common law. However clauses in agreements and meetings dictate whether certain information that is not readily available to the public and has been conveyed in confidence, is to remain confidential and not disclosed.

Personal Information includes information pertaining to employees, elected members, customers and residents/rate payers.

2.0 POLICY STATEMENT

2.1 Policy Provisions

- 2.1.1 Council will only collect information on members and staff members that it needs to carry out its functions and activities.
- 2.1.2 Council will only use information on members and staff for the purpose it was collected for.
- 2.1.3 Information on members and staff will only be disclosed for a purpose:
 - (a) that is directly and reasonably related to the necessary operations of the council or local government.
 - (b) if the member or staff consents to the use or disclosure; or
 - (c) if the disclosure is authorized by law.
- 2.1.4 Council must ensure contracts with third parties where the use of personal information is utilised must include provisions to protect the integrity and security of the personal information. Contracts must stipulate the contractor does not make unauthorised disclosures and may incorporate specific provisions about how the information is to be stored and disposed at the completion of the contracted activity.
- 2.1.5 Council is to take all reasonable measures to ensure the information it collects on members and staff members is accurate, complete and up to date.
- 2.1.6 Council will take steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 2.1.7 Council employees are responsible for protecting personal information from misuse, loss, corruption or disclosure. Personal information will be handled with care and only used for authorised purposes.
- 2.1.8 All employees must maintain public confidentiality and respect the privacy of individuals who have dealings with Council. Employees must treat all personal information as confidential and sensitive information as highly confidential. Council employees will not disclose any confidential information, use any information to their personal advantage or permit unauthorised access to such information.
- 2.1.9 Council files are strictly confidential and under no circumstances should a member of the public have access to files. Employees must also be conscious of security within the office

environment when members of the public are present. External customers must not be left unattended with Council files.

2.1.10 Destruction of records containing personal information, including personal records must be by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain. Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or the disintegration of paper. All computers that are removed from use and made available for non-Council purposes will have all data removed from the hardware.

2.2 Access and Correction to Data

2.2.1 Individuals are permitted to access information about them which is held by Council. Individuals are entitled to know generally what sort of information Council holds about them, for what purposes and how it collects, holds, uses and discloses that information.

2.2.1 Requests for access to such information are to be made in writing to the Director of Corporate Service. The Director of Corporate Services will establish the identity of the individual asking for the information.

2.2.2 Council will respond to public requests to correct information in a timely manner.

2.2.3 Council will provide written reasons when a request for access or correction of personal information is refused.

2.3 Confidential use of Media

BRC progressively install CCTV cameras on all BRC assets. The primary security use of CCTV is to discourage and/or detect unlawful behavior. CCTV can also help to improve perceptions of safety within the community by helping to prevent damage to property, deter anti-social behavior and inappropriate activity in settings such as libraries or leisure centers.

2.3.1 BRC expects authorised officers and stakeholders to ensure confidentiality of information gathered by or from CCTV operations, by not disclosing or discussing any events with unauthorized personnel or associates who have no direct responsibility relating to CCTV operations.

2.3.2 Treat all live and recorded images in an ethical manner and with the utmost of care, respect and dignity.

2.3.3 If access to CCTV footage is provided for an authorised purpose, a record is to be created by the officer processing the request, indicating the reason why the CCTV footage was extracted.

2.4 Anonymity

Whenever it is lawful and practicable to do so, customers will be given the option of not identifying themselves when dealing with Council.

2.5 Accounting privacy

2.5.1 Members, council staff and local government subsidiary staff have a right to privacy of their financial information as far as reasonably possible.

2.5.4 Council is to take all reasonable steps to maintain the privacy and integrity of the personal information it holds as part of its accounting records.

2.5.5 Council is to maintain a secure system for storing accounting records and related information on members and staff.

2.5.6 Appropriate access to accounting records by members and council staff as per schedule 1(8.2) of the Local Government Act 2019 Code of conduct.