# Privacy and Confidentiality Policy

## 1. Purpose

The purpose of this policy is to ensure that CQ Zero and its member organisations collect, store, share, and dispose of personal information in a lawful, ethical, and transparent manner. It establishes clear procedures that protect the privacy and confidentiality of individuals while supporting coordinated service delivery to end homelessness across Central Queensland.

This policy aligns with:

- *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles (APPs)*
- *Information Privacy Act 2009 (Qld)*
- *Human Rights Act 2019 (Qld)*
- *Interim Data Governance Provisions* adopted by Queensland's Zero communities

## 2. Scope

This policy applies to all CQ Zero staff, volunteers, contractors, partner organisations, and authorised users who collect, access, or share personal or sensitive information on behalf of CQ Zero.

It covers all forms of personal data, electronic and physical, collected through the:

- Australian Homelessness Vulnerability Triage Tool (AHVTT)
- By-Name List (BNL)
- CSnet AtoZ Database
- Service coordination meetings and related systems

## 3. Guiding Principles

CQ Zero upholds the following principles:

1. **Privacy and Confidentiality:** Personal information is handled in accordance with applicable laws and only for legitimate purposes related to CQ Zero's mission.

2. **Informed Consent:** Information is collected and shared only with explicit and voluntary consent, except where required by law.
3. **Purpose Limitation:** Data is used only for the purpose for which it was collected.
4. **Transparency:** Individuals are informed about how their information is used and who has access to it.
5. **Security:** Information is protected through secure systems, restricted access, and staff training.
6. **Accountability:** All staff and partners are responsible for protecting privacy and must report any breach immediately.

## 4. Collection of Personal Information

### 4.1 Informed Consent

- Consent must be obtained prior to collecting or sharing information using the AHVTT or similar tools.
- Individuals must understand:
  - What data is collected
  - Why it is collected
  - Who may access it
  - How it will be stored and shared
  - Their right to withdraw consent at any time

### 4.2 Types of Information Collected

CQ Zero may collect:

- **Personal Information:** name, contact details, date of birth, housing status.
- **Sensitive Information:** cultural background, health and wellbeing information, housing and service history, experiences of discrimination, and support needs.

### 4.3 Collection Method

Information is collected through trained case workers and stored securely in CSnet. Self-administered collection tools are not permitted.

# Privacy and Confidentiality Policy

## 5. Use and Disclosure of Personal Information

### 5.1 Purpose of Data Sharing

Data is shared to:

- Maintain and update the By-Name List.
- Coordinate housing, health, and support services.
- Track progress toward functional zero homelessness.
- Report deidentified, aggregate outcomes to funders and stakeholders.

### 5.2 Levels of Data Access

| Access Level | Description | Eligibility |
|---|---|---|
| **Level 1** | Direct access to input and update data in AtoZ (CSnet) | Selected housing/homelessness services engaging with high client volumes |
| **Level 2** | Access to client information through BNL coordination meetings | Partner services providing coordinated case support |
| **Level 3** | Deidentified data for reporting and advocacy | Public, government, research, and stakeholder use |

### 5.3 Authorised Data Sharing

Personal information may only be shared:

- With authorised CQ Zero member organisations that have signed a membership and confidentiality agreement;
- When required by law (e.g., mandatory reporting, court orders);
- For public reporting, only in aggregate and deidentified form.

# Privacy and Confidentiality Policy

## 6. Data Security and Confidentiality

### 6.1 Access Control

- Only authorised, trained personnel may access personal information.
- Access is role-based and recorded via audit trails in CSnet.

### 6.2 Secure Systems

- CSnet is the approved, encrypted database for all CQ Zero data.
- Information shared externally must use encrypted or password-protected files and secure email platforms.

### 6.3 Confidentiality Agreements

All staff and representatives must sign confidentiality and membership agreements prior to accessing data.

## 7. Data Retention and Disposal

- Personal information is retained only for as long as necessary to achieve CQ Zero's objectives or comply with legal obligations.
- Digital records are securely deleted from CSnet when no longer needed.
- Physical records are destroyed by shredding or secure destruction services.

## 8. Individual Rights

Under the *Privacy Act 1988* and *Information Privacy Act 2009*, individuals have the right to:

- **Access:** Request access to personal data held about them.
- **Correction:** Request correction of inaccurate or incomplete data.
- **Withdrawal:** Withdraw consent for ongoing sharing of their data (except where legally required).
- **Complaint:** Lodge a complaint if they believe their privacy has been breached.

# Privacy and Confidentiality Policy

Requests can be made in writing to the CQ Zero Project Lead. CQ Zero will respond within a reasonable timeframe.

## 9. Data Breach Response

In the event of a suspected or confirmed data breach:

1. **Immediate Containment:** Secure affected systems and restrict further access.
2. **Notification:** Inform the CQ Zero Project Lead and relevant parties.
3. **Assessment:** Determine the scope, cause, and potential harm.
4. **Notification to Individuals:** Notify affected persons if there is risk of serious harm.
5. **Reporting:** Notify the Office of the Australian Information Commissioner (OAIC) if required under the *Notifiable Data Breaches Scheme*.
6. **Remediation:** Implement corrective and preventive measures.

## 10. Training and Compliance

- All staff and partner organisations must complete privacy and data security training annually.
- Regular audits will be conducted to ensure compliance with privacy obligations and system security protocols.
- Breaches of this policy may result in disciplinary or contractual consequences.

## 11. Review and Updates

This policy will be reviewed annually or when relevant legislation or organisational practices change.