1. **Title**: **Information Privacy Policy**

2. **Purpose:**

The Queensland Information Privacy Act 2009 (the IP Act) provides a right for individuals to have their personal information collected and handled in accordance with 11 Information Privacy Principles. These Privacy Principles apply to Queensland Government agencies such as Community Enterprise Queensland (CEQ).

CEQ's Information Privacy Policy provides safeguards for the handling, access and amendment of personal information.

3. **Scope:**

This policy applies to all team members, Board of Management members, contractors and volunteers of CEQ. This policy applies to the collection of personal information, regardless of when it came into existence, and to the storage, handling, accessing, amendment, management, transfer, use and disclosure of personal information regardless of when it was collected.

4. **Background:**

CEQ's functions require the collection, creation, use and in some circumstances the disclosure of personal information about team members, customers, stakeholders and the public. CEQ is committed to protecting personal privacy and recognises that team members, customers, stakeholders and the public have a reasonable expectation that CEQ will protect and appropriately manage the personal information it holds about them.

Aligned with the Act and the CEQ principles of Respect for Persons, Integrity and Diligence, CEQ team members have a responsibility to respect the personal information CEQ collects and holds.

Additionally, under the Human Rights Act 2019, public entities must act compatibly with human rights and give them proper consideration before making a decision. The rights set out in the Human Rights Act include a right to privacy. When carrying out their functions, in addition to meeting their obligations under the Information Privacy Principles, CEQ and its team members will recognise, and act compatibly with, this right to privacy.

5. **Roles and Responsibilities:**

5.1 **The CEO** - The Chief Executive Officer (CEO) is the Principal Officer under the IP Act and has overall responsibility for CEQ's obligations under the Act.

5.2 **General Manager Corporate Services -** The General Manager Corporate Services oversees implementation of privacy management across CEQ, and approves privacy protocols, guidelines and mandatory training arrangements.

5.3 **Audit, Risk & Procurement Manager** - As the Privacy and Data Protection Officer, the Audit, Risk and Procurement Manager is responsible for determining the outcome of IP Act applications and administering the IP Act on behalf of CEQ including:

(a) managing privacy risk in the organisation and implementing business processes consistent with the IP Act;

(b) managing access and amendment applications under the IP Act;

(c) liaison with both prospective applicants and CEQ team members regarding access to documents;

(d) advising team members on CEQ's privacy obligations; and

(e) coordination of CEQ's investigation and response to privacy complaints.

5.4 **Information Technology Manager** – Acts as the Personal Information and Data Custodian and is responsible for:

(a) implementing reasonably practical security measures to protect privacy of personal information in information systems;

(b) determining user access levels which must be consistent with privacy requirements; and

(c) implementing appropriate mechanisms to revoke access to systems containing personal information, when access is no longer appropriate, for instance, in the case of a change in position or formal responsibilities, or termination of employment.

6. Collection and Management of Personal Information

6.1 This Policy applies to the collection, use, storage, transfer, handling, right of access, and amendment of personal information at CEQ. It does **not** apply to:

(a) the Act includes an exemption for routine employment information of team members;

(b) personal information which is maintained on a public register;

(c) information recorded in a de-identified way which cannot be linked (or re-linked) to a known individual;

(d) personal information which is already available in a publication or other publicly available document; or

(e) information which is generally available.

6.2 There must be a lawful purpose for collecting personal information, and that the purpose is related to the functions or activities of CEQ;

6.3 The individual who provides the information is aware of the purpose for which the information is being collected;

6.4 Information must be stored securely;

6.5 Subject to certain exceptions, CEQ must provide individuals with access to personal information about them and correct the information they hold to ensure that it is accurate, up to date, relevant, complete and not misleading;

6.6 CEQ must seek an individual's permission to use or disclose personal information for a purpose that is not directly related to the purpose for which it was collected;

6.7 Day-to-day access to the personal information of others is restricted to team members in the organisational unit that requires access e.g. Human Resources team members have access to employment records (role-based access). Team members must only access personal information if there is a work-related reason for this.

6.8 Deliberate misuse, unauthorised access or inappropriate access by team members is prohibited.

6.9 Team members must not disclose personal information to individuals or organisations outside of CEQ. Disclosure refers to release of personal information to another entity (e.g. a body, agency or person separate from CEQ) where CEQ will cease to have effective control of the information once it is released;

6.10 CEQ will take all reasonable steps to ensure that third party service providers do not use or disclose transferred personal information for a purpose other than that for which it was collected by CEQ. CEQ will do this primarily by entering into legally binding contracts with service providers which require compliance with the Information Privacy Principles contained in the IP Act and/or Privacy Act (where applicable);

6.11 CEQ may disclose confidential information to a Minister, their advisors or Parliament or its Professional Advisors if requested;

6.12 Tax File Number Guidelines 1990 must be adhered to;

6.13 Law enforcement agencies are not subject to IPP's if that agency is satisfied that non-compliance is necessary. Law enforcement areas of government (e.g. the Queensland Police Service or the Crime and Corruption Commission) that find, prevent, detect, investigate and take offenders to Court, are permitted to not follow some of the privacy principles in certain circumstances, as long as they are satisfied on reasonable grounds that it is necessary;

6.14 The Act includes a list of documents that the privacy principles do not apply to. It does not matter which area of Government holds these documents; they will always be exempt from the privacy rules. They are documents about:

(a) covert activity;

(b) witness protection;

(c) disciplinary action and misconduct;

(d) public interest disclosure;

(e) the cabinet and executive council; and

(f) commissions of inquiry.

Collection and Processing of Sensitive Information

Sensitive information is personal information relating to an individual's:

- health
- racial or ethnic origin, including country of birth;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;

- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices;
- criminal record; and
- child related employment screening reports.

CEQ will only solicit and collect sensitive information if:

(a) it is required to do so by law; or

(b) it has the explicit consent of the individual to whom the information relates, and it is reasonably necessary for CEQ to collect the sensitive information to enable it to carry out a relevant function or activity; or

(c) processing is necessary to protect the vital interests of the individual or of another person (being those essential to sustaining their life) where the individual is physically or legally incapable of giving consent; or

(d) processing relates to personal data which is in the public domain; or

(e) processing is necessary for the establishment, exercise or defence of legal claims; or

(f) processing is necessary for public interest reasons in the area of public health.

Electronic data storage

CEQ is committed to ensuring that the information it receives is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure. CEQ aligns itself with the Government-recommended 'Essential 8' security framework and adopts a 'Zero Trust' network architecture. The Essential 8 is a set of recommended cybersecurity strategies developed by the Australian Cyber Security Centre (ACSC) to help organisations protect against cyber threats. Zero Trust is a security model based on the principle of "never trust, always verify." This means that no user or device is trusted by default, even if they are inside the network perimeter.

CEQ Source Data Residency Matrix

	Office365					CSX (Datacentre)			Internet Facing										
GEO	AU	AU	AU	AP	US	AU	AU	AU	AU	AU	AU	AU	AU	AU/US	US	US	US	IRE	AU
Access Method	MFA	MFA	MFA	MFA	MFA	WAN	WAN	WAN	n/a	MFA	Pword	MFA	Pword	Pword	Pword	Pword	Pword	Pword	Pword
Technology	Sharepoint	Ondrive	Email	Teams	Yammer	Pronto	File Server	Sharepoint	CEQ Website	Convene	Promaster	Sharefile	Humanforce	seek.com.au	mailchimp	SafetyCulture	Culture Amp	HappyOrNot	NAB
Source Data																			
Customer Website Submissions			•						•						•			•	
Christmas Club Customer Data			•			•	•												•
Supplier Details			•			•	•				•	•							
Contractor Details			•			•	•					•							
Online Job Applications			•				•							•					
Customer PII Data			•			•	•												
Employee PII Data	•		•	•	•	•	•	•			•		•			•			
CEQ Documents	•	•	•	•	•		•	•		•	•	•				•		•	
Annonymous Survey Results																	•		

7. Privacy complaints or breaches:

Complaints

If an individual believes that CEQ has not dealt with their personal information in accordance with the IP Act or this Policy, they may make a complaint. A complaint must be made in writing or by email to the Privacy and Data Protection Officer at feedback@ceqld.org.au.

Primary responsibility for investigating and responding to the complaint will rest with the General Manager of the business unit concerned, with advice from the Privacy and Data Protection Officer as required. CEQ's main objective in responding to privacy complaints is to conciliate an outcome which is acceptable to the complainant and which addresses any broader or systemic privacy issues which may arise.

If a complainant does not agree with the CEQ's response, an internal review process is available or a complainant may refer the matter for independent mediation by the Office of the Information Commissioner.

IP Act or Policy Breaches

Breaches of the IP Act or this Policy must be reported to the Privacy and Data Protection Officer as soon as practicable. A Policy breach that alleges deliberate misuse, unauthorised access or inappropriate access to personal information by a CEQ team member may be grounds for misconduct/serious misconduct and may result in disciplinary action.

The General Manager of the relevant business unit must report any privacy breaches to the Privacy and Data Protection Officer as soon as the breach has been identified. Management of a privacy breach will include steps to:

(a) contain the breach;

(b) evaluate the associated risks;

(c) consider notifying the affected individuals; and

(d) ensure prevention of any further privacy breach.

The CEO must be informed of serious breaches of this Policy and any actions arising out of any investigations into a breach.

For a Notifiable Breach, CEQ is obligated to inform the Australian Information Commissioner and particular individuals about eligible data breaches in accordance with the IP Act Personal Information – Data Breach Procedure.

8. Associated Documents:

CEQ Code of Conduct; CEQ Conflict of Interest Policy; CEQ Right to Information Policy; Information Privacy Act 2009; Human Rights Act 2019; *Information Privacy Principles,* Office of the Information Commissioner; Essential 8 cybersecurity strategies developed by the Australian Cyber Security Centre (ACSC).

9. Approved by:

Michael Dykes
Chief Executive Officer Date: 17/07/2024 Review Date: 17/07/2027