Policy: Privacy Policy

1. Policy

This policy outlines how Incite Collective collects, stores, uses, discloses, and safeguards personal information. It also explains individuals' rights regarding their information and how to raise concerns or request access or correction.

2. Purpose

This policy outlines how Incite Collective collects, stores, uses, discloses, and safeguards personal information. It also explains individuals' rights regarding their information and how to raise concerns or request access or correction.

3. Scope

This policy applies to all personal information collected by Incite Collective in connection with its operations, including support coordination, psychosocial recovery coaching, training, advocacy, and stakeholder engagement activities.

4. Policy Statement

Incite Collective is committed to protecting the personal information of all participants, staff, contractors, and stakeholders. We value the privacy, dignity, and autonomy of every individual and are dedicated to handling personal information in a lawful, transparent, and respectful manner, in line with the **Queensland Privacy Principles (QPPs)** under the **Information Privacy Act 2009 (as amended by the IPOLA Act 2023)**.

5. What is Personal Information?

'Personal information' refers to any information or opinion, whether true or not, about an identified individual or someone who is reasonably identifiable. This includes names, contact details, health or support information, and cultural, behavioural, or psychosocial data.

6. Our Privacy Obligations

- Incite Collective is bound by the 13 Queensland Privacy Principles (QPPs), which govern:
- Open and transparent management of personal information;
- Collection, use, and disclosure of information;
- Data security and accuracy;
- Access and correction rights;
- Cross-border disclosures.
- We also comply with relevant NDIS Quality and Safeguarding Framework standards.

7. How we Collect Information

We collect personal information in the following ways:

- Directly from individuals (e.g., intake forms, emails, phone calls, meetings);
- From third parties with consent (e.g., family, support networks, service providers);
- Through our website and digital platforms (limited to contact forms and secure portals).

8. Why We Collect Personal Information

We collect information to:

- Deliver high-quality, person-centred services to NDIS participants;
- Support safe and ethical practice;
- Meet our legal, regulatory, and reporting obligations;
- Improve our services through feedback and evaluation.

We only collect personal information necessary for our functions and will not use it for secondary purposes without consent unless authorised by law.

9. Use and Disclosure

We may disclose personal information:

- To participants or their nominated representatives;
- To service providers, government agencies, or advocates (with consent);
- Where required or authorised by law;
- In circumstances involving serious threats to health, safety, or welfare;
- As required under the Mandatory Data Breach Notification Scheme.

We do not sell or rent personal information to third parties.

10. Cross-Border Disclosure

We may disclose personal information:

- To participants or their nominated representatives;
- To service providers, government agencies, or advocates (with consent);
- Where required or authorised by law;
- In circumstances involving serious threats to health, safety, or welfare;
- As required under the Mandatory Data Breach Notification Scheme.

We **do not sell or rent** personal information to third parties.

11. Data Quality and Security

We are committed to maintaining the accuracy and security of personal information. We:

- Regularly review and update records;
- Use secure systems and access controls;
- Train staff on privacy obligations;
- Limit access to authorised personnel only.

12. Access and Correction

You have the right to request access to your personal information and ask for corrections if it is inaccurate, incomplete, or out of date. To do so, contact us using the details below. We will respond within a reasonable time and may request verification of your identity.

13. Mandatory Data Breach Notification

Under the IPOLA Act, we are required to notify the Office of the Information Commissioner (OIC) and affected individuals if a data breach is likely to result in serious harm. We will:

- Contain the breach;
- Assess the risk;
- Notify those impacted;
- Review our processes to prevent recurrence.

Please refer to our Data Breach Response Policy.

14. How to Make a Complaint

If you believe we have breached your privacy or mishandled your information:

1. Contact us directly using the details below.
2. We will respond within 30 days.
3. If unresolved, you may lodge a complaint with the Office of the Information Commissioner Queensland.

15. Policy Dissemination:

16.

This policy will be communicated to all Incite Collective Members. It will be accessible through organisation communication channels and other appropriate means.