1 Introduction

This Policy sets out the policies relating to the privacy and confidentiality relating to all personal information within InsideOut Pathways Inc ("**IOP**"). All IOP Members and non-Member Volunteers are to comply with this policy.

IOP respects your privacy and is committed to protecting the personal information we collect.

This Privacy Policy explains how we collect, use, disclose, and protect personal information in accordance with the updated Australian Privacy Principles under the *Privacy Act 1988 (*Australia*)*, as amended by the *Privacy and Other Legislation Amendment Act 2024* (Cth).

It also explains how we may use artificial intelligence ("**AI**") and automated systems when providing our services.

The IOP Management Committee ("**IOP-MC**") are accountable for managing this policy within IOP.

2 Changes to this Policy

We may update this Privacy Policy from time to time.

The latest version will always be available on our website.

3 Overview

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.

IOP receive and maintain sensitive personal information of IOP Members, IOP Non-Member Volunteers and potential, current and past clients ("**Clients**") including, but not limited to:

(a) Name, address and contact details;
(b) Date of birth;
(c) Next of kin details;
(d) Medical conditions and health information;
(e) Criminal background and history;
(f) Identification details (drivers licence/passport etc);
(g) Bank account details;
(h) Photographs;
(i) File notes relating to individuals;
(j) Email correspondence;
(k) Incident/Accident claim correspondence; and
(l) Criminal History Record correspondence.

3.2 Health Information

As part of administering IOP and providing IOP services, we may collect or be privy to health information and other sensitive information. For example, IOP may collect or be privy to criminal background and history information from current or ex-prisoners to advise and assist them on the IOP services required.

Sensitive information includes the following type of information: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or associations; philosophical beliefs; memberships; sexual orientation; genetic information; biometric information; biometric templates. IOP will limit the collection of sensitive information to the minimum amount required to perform our services.

3.3 Information Storage and disposal

Personal Information is in most cases kept in soft copy in a cloud-based storage facility with access only to IOP core members. Local synchronised copies of the cloud storage may exist on IOP members local storage or network access storage (NAS).

Some information is kept in emails on IOP members local PC storage or Cloud services such as Gmail, Hotmail, smartphones, iCloud, Google Drive etc.

In addition, some Personal Information is stored on IOP web services and available through private web sites which may be hosted overseas by third parties and access protected with username/passwords. The IOP public website and other materials may display photos and names of members and clients, published with permission.

4 Policy

IOP will endeavour to handle Personal Information in accordance with this Privacy Policy and the Australian Privacy Principles.

This Privacy Policy summarises how IOP handles personal information. We may revise this Privacy Policy from time to time. The revised Privacy Policy will take effect when it is published to members and posted on the IOP website.

5 Privacy and Confidentiality

When handling financial and personal information about clients or others with whom IOP has dealings, members must observe the following principles:

(a) Collect, use, and retain only the personal information necessary for IOP's business. Whenever possible, obtain any relevant information directly from the person concerned.

(b) Retain information only for as long as necessary or as required by law. Protect the physical security of this information.

(c) Limit internal access to personal information to those with a legitimate business reason for seeking that information. Use only personal information for the purposes for which it was originally obtained. Obtain the consent of the person concerned before externally disclosing any personal information, unless legal process or contractual obligation provides otherwise.

(d) First discuss any concerns or suggestions to improve the service we provide to the client with a committee member

6 Breach Risks and Mitigation

IOP mitigates breaches of Privacy by adopting the following actions:

(a) The use of strong passwords and Multi-Factor Authentication.

(b) Education of all members – including through the Code of Conduct.

(c) Monitoring and tracking for breach.

(d) Encourage breach reporting to IOP Management Committee.

7 Breach Management and Reporting

In the event of a privacy breach being identified, the IOP-MC will allocate a Breach Manager to investigate and mitigate the breach, reporting to the IOP-MC in a timeframe determined on a case by case basis.

Where criminal activity may be suspected, the relevant statutory authority will be informed, and IOP will fully cooperate with all authorities.

IOP is currently not large enough for mandatory privacy breach reporting to the authorities.

8 Complaint Management

If you have any queries or would like to make a complaint regarding relating to our Privacy Policy or how we handle your personal information, please contact us using the details in Section 10 - Contact Us. We endeavour to respond to complaints and queries within fourteen calendar days of their receipt. If you are dissatisfied with our response, you may refer the matter to the Australian Information (Privacy) Commissioner (see www.oaic.gov.au).

If you do not provide some or all of the personal information requested, we may not be able to offer you services or provide you with information about our causes, events, programs and projects.

9 Website usage information and cookies

When you access our website, we may use software embedded in our website (such as PHP and Javascript) and we may place small data files (or cookies) on your computer or other device to collect information about which pages you view and how you reach them, what you do when you visit a page, the length of time you remain on the page, and how we perform in providing content to you.

A cookie does not identify individuals personally, but it does identify computers. You can set your browser to notify you when you receive a cookie and this will provide you with an opportunity to either accept or reject it in each instance.

We may gather your IP address as part of our business activities and to assist with any operational difficulties or support issues with our services. This information does not identify you personally.

We may use Google Analytics features based on Remarketing, Google Analytics Demographics, and Interest Reporting. These features use first party and third-party cookies to inform and optimise content based on your past visits to our site.

We may also use pixel tracking, which indicates when your computer has visited pages on our websites where a pixel has been installed. As with cookies, this does not identify you personally, only the device you are using.

Google Analytics informs us of how visitors use our site based on your browsing habits, so that we can improve our site to make it easier for you to find the information you are seeking. Google also receives this information as you browse our site and other websites on the Google Display Network using Remarketing.

You can use the Google Analytics Opt-out Browser Add-on so you are not tracked into Google Analytics.

9.2 Cross-border disclosures of your personal information

We use data hosting facilities and third-party service providers to assist us with providing our goods and services. As a result, your personal information may be transferred to, and stored at, a destination outside Australia, including but not limited to New Zealand, Netherlands, China, Singapore, Hong Kong, Ireland, Canada, United States of America and the United Kingdom.

Personal information may also be processed by staff or by other third parties operating outside Australia who work for us or for one of our suppliers, agents, partners or other support networks associated with IOP. We take such steps as are necessary in the circumstances to ensure that any overseas third-party service providers we engage do not breach the Australian Privacy Principles, including through contractual arrangements.

If your personal information is collected using a collection notice that references this Privacy Policy, you are taken to consent to the disclosure, transfer, storing or processing of your personal information outside of Australia. You also acknowledge and understand that by providing such consent that we will not be required to take such steps as are reasonable in the circumstances to ensure such third parties comply with the Australian Privacy Principles.

9.3 Disclosure that Artificial Intelligence (“AI”) is used

For transparency, IOP advise that we may use artificial intelligence and automated systems to assist in analysing information, improving our services (including marketing materials, training materials,

web site and social media content) and supporting decision-making processes. AI is also used in the development of marketing materials including the IOP website.

These systems may help us:

(a) Analyse information;
(b) Match individuals with opportunities;
(c) Provide automated responses (such as chatbots);
(d) Detect fraud or misuse; and
(e) Improve service delivery and efficiency.

AI tools may analyse Personal Information you provide in order to generate insights or recommendations.

Where appropriate, important decisions are reviewed by a human, usually the IOP-MC.

Information used by AI systems may be aggregated or de-identified to improve system performance.

No in-house developed AI systems are used. IOP generally use AI services such as Gemini (Google), ChatGPT and similar.

9.4 General Data Protection Regulation (GDPR)

IOP has no plans to market to the European Union, nor use suppliers from countries using GDPR. Accordingly, IOP is not adopting GDPR principles, instead relying on the Australian Privacy Principles. Should this situation change, this policy will be updated.

10 Contact Us

If you have any questions about this Privacy Policy or our handling of personal information, please contact us:

InsideOut Pathways Inc.

Email: secretary@iop.org.au

Phone: 0466 818 706

Address: PO Box 307, Samford LPO, Queensland 4520, Australia.