PORT PHILLIP COMMUNITY GROUP // Working for Social Justice	Policy number: 1.6	Privacy	Version (review)	2.2
	Drafted by	Karen Sait (EO)	Approved by Board on	May 2021
	Responsible Person	Board and EO	Scheduled review date	May 2024

PRIVACY POLICY AND PROCEDURES

1. PURPOSE AND SCOPE

PPCG recognises and respects every person's right to privacy, dignity and confidentiality. This policy outlines PPCG's commitment to protect the privacy of personal and sensitive information of our clients, staff and volunteers.

This policy applies to all PPCG staff, Board Directors, clients, contractors, students and volunteers.

2. POLICY

PPCG is committed to complying with the relevant privacy legislation including the:

- ***Privacy and Data Protection Act*** 2014 (Vic) and its 10 Information Privacy Principles.
- ***Privacy Act*** 1988 (Cth).
- ***Victorian Freedom of Information Act*** 1982.

PPCG seeks to uphold the highest standard of privacy by:

- Protecting a client's right to privacy.
- Creating an environment in which clients are confident that their rights are protected.
- Guiding the fair and responsible handling of client information.
- Protecting the privacy of information.
- Providing individuals with a right of access to their own information.
- Requiring all PPCG workplace participants to sign the PPCG Code of Conduct stipulating they must:
  - protect the privacy of others and maintain appropriate confidentiality regarding personal matters and PPCG material.
  - comply with additional conduct requirements stipulated in policies, agreements, awards and professional associations.

3. DEFINITIONS

Term	Definition
Client (aka as 'Service User' or as a 'Consumer' for the purposes of this document)	Any individual receiving or participating in any of PPCGs programs, classes, courses, activities, initiatives and/or events.
Staff Member	Refers to PPCG workplace participants including staff, board, volunteers and students (workplace participants)
Freedom of Information Act	The ***Victorian Freedom of Information Act*** 1982 gives consumers the right to request information held by Ministers, State Government departments, local councils, public hospitals, most semi-government agencies and statutory authorities. The Act gives consumers the right to access documents about their personal information and the activities of government agencies along with the right to request that incorrect or misleading information held by PPCG may be amended or removed.

Information Privacy Principles	The 10 Information Privacy Principles are the core privacy law in Victoria and set out the minimum standard for how Victorian public sector bodies manage personal information.
Office of the Victorian Information Commissioner (OVIC)	Independent regulator with combined oversight of information access, information privacy and data protection.
Personal Information	Recorded information or opinion, whether true or not, about a person whose identity is apparent, or can reasonably be ascertained, from the information. The information or opinion can be recorded in any form. For clarity, we use the words 'personal information' to include personal information and health information. PPCG does not intentionally collect health information but we may receive it in the course of our normal business processes.
Privacy	Privacy is a human right and information privacy (being the protection of personal information) is a key aspect of this right.
***Privacy and Data Protection Act* 2014 (Vic) (PDP Act)**	Provides for the regulation of information privacy, protective data security, and law enforcement data security to undertake research, issue reports, guidelines and other materials with regard to information privacy (excluding health information).
The Executive Officer (EO) is also the Privacy Officer	PPCG has a designated person within an organisation that is responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to policies and procedures relating to privacy, access, and client information in compliance with legislation.
Sensitive Information	Sensitive information means information or opinion (that is also personal information) about a person's racial or ethnic origin, political opinions, religion, philosophical beliefs, sexual preferences or practices, membership of a political association, professional/trade association or trade union, or an individual's criminal record.
Subpoena	A legal document that commands a person or entity to testify as a witness at a specified time and place (at a deposition, trial, or other hearing), and/or to produce documents or other tangible objects in a legal proceeding.

4. PRINCIPLES

This Privacy Policy is based on the 10 Information Privacy Principles (IPPs) which are the core of privacy law in Victoria and set out the minimum standard for how Victorian public sector bodies should manage personal information.

The IPPs are contained in Schedule 1 of the ***Privacy and Data Protection Act 2014*** (Vic) and are available at: https://ovic.vic.gov.au/wp-content/uploads/2018/07/Guidelines-to-the-IPPs-2011.pdf.

Each principle is detailed below.

Principle 1: Collection of Data

PPCG collects a variety of information required to provide services to our clients.

PPCG will not collect information about an individual unless it is necessary and/or:

- The individual has provided consent.
- The information is necessary to prevent or lessen a serious and imminent threat to the life, health, safety or welfare of any individual, or a serious threat to public health, public safety or public welfare PPCG is required to collect the information by law.

When PPCG collects information from an individual, PPCG staff will inform the individual:

- The reason why PPCG is collecting this information and the purpose for which the information is collected.
- To whom PPCG shares information with and the procedure for sharing information.
- The main consequences (if any) for the individual if all or part of the information is not provided.
- The identity of PPCG and how to contact us.

Principle 2: Use and Disclosure of Data

PPCG only uses and discloses information for the primary purpose for which it was collected or a related secondary purpose. This includes:

- Assessing eligibility and access to our services.
- Adapting services to meet client needs.
- Seeking client feedback.

PPCG will only disclose information to third parties without client consent, in the following circumstances:

- Sharing information will prevent or minimise serious and imminent harm to the individual or others.
- Where the use or disclosure is required by law.

If PPCG uses or discloses information where consent is required, without obtaining this consent, this is considered a Privacy Breach.

This policy recognises that client information held by PPCG may be sensitive. Where a staff member has any concerns about a use and disclosure of data they should speak to their Manager or to the EO.

Principle 3: Data Quality

PPCG is committed to ensuring that the information it holds is accurate, complete and up to date.

Training and audits are conducted regularly to support this.

Principle 4: Data Security (and Data Retention)

This principle contains two distinct obligations. The first deals with data security, requiring organisations to protect information they hold. The second deals with the disposal of data, requiring organisations to destroy or de-identify information they no longer need.

In relation to data security, PPCG:

- Is committed to protecting the information it holds and will implement measures to protect information from misuse, unauthorised access, change or disclosure.
- Will destroy or permanently de-identify information when no longer needed or it is no longer required to be kept for legal purposes.
- Will take reasonable steps to protect the security of your information.

- PPCG uses a combination of people, processes and technology safeguards across information, ICT, personnel and physical security to protect information from misuse and loss, and unauthorised access, modification and disclosure.

Physically Securing Client Records

- During office hours when staff are not in attendance in their offices, all client records or information are to be kept out of sight, in a secure location (e.g., behind a locked door or in a drawer). It is the responsibility of the staff member to ensure files in their possession are kept safely and confidentially.
- Client records are to be returned to the central client records storage area at each site at the end of the day and are locked away overnight.
- Records carried on home visits, are to be kept in a locked briefcase and carried with staff at all times. They are not to be left in cars or taken home.
- Personal information that does not need to be kept (e.g. photocopies or professional diaries) is to be permanently destroyed, usually by shredding.
- All discussions about clients, whether they are between staff within the organisation, or on the phone, must occur in a confidential environment (i.e. in offices, not in reception, corridors or the staff room).

Email and Electronic Transmission

After a client has consented to release information and this is documented in the client record, personal client information may only be transmitted electronically by:

- e-referral systems
- Secure email of a PDF file;
- Facsimile. When emailing/faxing client information, PPCG will take reasonable steps to ensure information is secure from loss, unauthorised access and modification

Using Secure Email

PPCG will take “reasonable” steps to keep information safe when transmitting it outside the organisation. One or more of the following steps can be taken to keep email safe:

- Email only PDF versions of text and image documents
- Convert PDF documents to un-editable format where available
- Check PDF files have converted correctly and all pages are correct before sending
- Password protect the PDF file
- Call the intended recipient before sending to alert them to the fact the email is coming – either give the file password here or send via separate email
- Check that “addresses” on emails and faxes match intended recipients before sending
- Activate the “read receipt” option in email software before sending
- Add to progress notes that the email/facsimile was received correctly
- Follow-up emails/faxes not confirmed as received

Further Steps to Securing Email

PPCG will:

- Minimise external or remote access to unencrypted emails on server (firewalls, police checks of IT staff/contractors)
- Minimise the number of internal staff that have server access to unencrypted emails
- Oversee contractor access to unencrypted server emails and take steps to minimise unauthorised access or copying
- Add suitable disclaimers/warnings to email footers of all staff

Principle 5: Openness

PPCG will:

- Ensure clients are aware of PPCG's Privacy Policy and its purposes.
- Make this information freely available in relevant publications and on the organisation's website, on noticeboards and via PPCG Information Brochures (*pending the development of a dedicated Privacy Brochure*).

Principle 6: Access and Correction of Data

PPCG will ensure individuals have a right to seek access to information held about them and to correct inaccurate, incomplete, misleading or not up to date.

Principle 7: Unique Identifiers

PPCG does not assign unique identifiers to individuals. Each request for service, enquiry or complaint that PPCG receives is given a number so that it can be managed efficiently, but not each individual. PPCG will not request a unique identifier created by another organisation unless required by law, nor will PPCG use or disclose a unique identifier created by another organisation unless there is a lawful basis for doing so.

Principle 8: Anonymity

PPCG wherever lawful and practicable, will provide individuals with the option of non-identifying themselves. This includes allowing people from whom the personal information is being collected to not identify themselves or to use a pseudonym unless it is impracticable to deal with them on this basis.

Principle 9: Trans Border Data Flows

PPCG will only transfer information outside of Victoria if that data transfer conforms to the reasons and conditions outlined in the Act.

Principle 10: Sensitive Information

PPCG will only collect sensitive information if:

- The individual gives consent
- Required or authorised under law
- Necessary to lessen or prevent a serious threat to the life or health of any individual
- Necessary for legal or equitable claims.

PPCG will comply with any lawful and reasonable requests for information from statutory bodies.

Privacy Breaches

Responding to a privacy breach quickly and efficiently can substantially decrease the impact of a breach on individuals, reduce the costs associated with dealing with a breach, and reduce the potential damage that can result from a breach.

Where a real or suspected privacy breach is identified, the relevant PPCG Manager should be informed so that an initial assessment can be undertaken to determine next steps or corrective action. All efforts will be made to contain a privacy breach and corrective actions will be implemented and monitored. Where a breach relates to Client/Service User Information, the relevant PPCG Manager or the Executive Officer will consider mitigation strategies including whether full disclosure and apology is required for serious breaches.

Providing disclosure about low-risk breaches can cause undue anxiety and de-sensitise individuals to disclosure. Each incident needs to be considered on a case-by-case basis to determine whether breach disclosure is required.

INFORMATION REQUESTS

Any enquiries regarding the privacy of information should be directed to:

The Port Phillip Community Group Executive Officer

Post: PPCG Executive Officer
Port Phillip Community Group
161 Chapel Street
St. Kilda 3182

Email: info@ppcg.org.au

If the matter is a complaint about the way information was handled, it will be handled as per PPCG's ***Service User, Client, Carer and Community Feedback Procedure***.

If a client believes that PPCG has breached their privacy they can lodge a complaint and all attempts will be made to resolve the situation.

The complaint will be addressed by the Executive Officer and outcomes reported to the complainant.

The Executive Officer will make a summary report of the complaint and outcome to the Board of Directors.

If a client is still not satisfied with the outcome they may refer the matter to the Office of the Victorian Information Commissioner.

Office of the Victorian Information Commissioner

Post: Office of the Victorian Information Commissioner
PO Box 24274
Melbourne VIC 3001

Email: enquiries@ovic.vic.gov.au

5. RELATED DOCUMENTS

- *PPCG Code of Conduct*
- *Service User, Client, Carer and Community Feedback Policy and Procedure.*
- *Records Management Policy.*
- *Client Rights and Responsibility Brochure/Privacy Brochure.*

6. DOCUMENT HISTORY

(Note: Next review due as per Policy Review Schedule)

Action	Date	Responsibility	Approved by
Initial Issue	2003	EO	Board of Directors
Review	May 2021	EO	Board of Directors