VICTIMS & WITNESSES of CRIME COURT SUPPORT

PRIVACY POLICY

Purpose

The purpose of this policy is to outline how VWCCS complies with the principles outlined in the Commonwealth Privacy Amendment (Enhancing Privacy Protection Act) 2012 and the Australian Privacy Principles updated July 2022.

In Australia, the privacy laws generally relate to the protection of an individual's personal information. Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable – it is anything that tells us about who you are.

Key Message

This policy provides a consistent and transparent process for managing the personal information of:

- Current and former VWCCS volunteers
- Current and former clients of VWCCS including client information from Referral Agencies

It clearly explains how we handle personal information.

Date published: November 2024 Review date: December 2025

VWCCS approach to Privacy

VWCCS is committed to protecting the privacy of all volunteers and clients and being open and transparent about how personal information is handled.

This HR Privacy Policy applies to all staff, volunteers, Board Members of VWCCS and contractors.

Purpose of this Privacy Policy

The purpose of this policy is to protect Personal Information about current or former volunteers and clients, and to ensure that VWCCS complies with the Privacy Act and the Australian Privacy Principles

Contact: If you have questions relating to this policy please address them to the General Manager

Volunteers and staff are requested to email VWCCS at info@vwccs.org.au Attn: General Manager if their Personal Information is inaccurate or incomplete. Requests will be responded to within 30 days and all reasonable efforts will be made to correct Personal Information subject to VWCCS record retention obligations.

VICTIMS & WITNESSES
of CRIME COURT SUPPORT

Section One: Volunteers and Staff

Kinds of Personal Information about Volunteers that VWCCS collects

VWCCS may collect Personal Information about Volunteers and staff either in paper or in electronic format including (but not limited to) all or any of the following:

- Personal and emergency contact details including names, date of birth, email, telephone numbers, address and postal address.
- Emergency contacts.
- Resume and covering letter.
- Details of previous employment and references.

Reasons for Collecting Personal Information on Volunteers

Personal Information of prospective and current Volunteers is collected as part of maintaining the organisation's relationship with them. This includes for:

- Recruitment.
- Appraising performance or conduct.
- Assessing ability to perform duties.
- Investigating possible employee fraud including unauthorised access.
- Obtaining and maintaining security clearances.
- Conducting pre-employment and ongoing police, medical and working with children checks.
- Managing emergencies.

Collection of VWCCS Volunteer and Staff Personal Information

Personal Information may be collected:

- When applicants seek to become a volunteer or a staff member.
- Upon acceptance of a position of volunteer or staff member with VWCCS.
- Throughout the time as a volunteer or staff member to update details.
- Upon termination.

VWCCS will only collect Personal Information directly from the volunteer or staff member to whom the information relates.

Use of Volunteer and Staff Personal Information

VWCCS will not use volunteer or staff Personal Information for a purpose other than that for which it was collected unless:

- The use of the Personal Information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the Personal Information relates or of another person; or

- If so directed by a court of law, law enforcement agency or authorised regulator.

If VWCCS uses or discloses Personal Information (authorised above), it will make a written note of the use of disclosure and of the reason for its disclosure.

Disclosing Volunteer and Staff Personal Information to Other Parties

VWCSS will not disclose Personal Information to anyone or any organisation, unless:

- The disclosure is related to the purpose for which the information was collected.
- The disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person.
- In relation to some investigations and law enforcement process; or
- Legislation recognises lawful access by some government agencies.

How Volunteers and Staff may Access, Update, and Correct Personal Information

Volunteers and staff are entitled to access Personal Information that VWCCS holds. (see "Contact' in the introduction if you have questions about accessing your information)

Volunteers and staff will be given full access to the following types of Personal Information using a method appropriate to the circumstances e.g. providing a copy or citing the documents/information:

- The terms and conditions of engagement.
- Personal and emergency contact details.
- Information relating to performance of their role.

Update/Correction Requests

VWCCS will take all reasonable steps to ensure that any Personal Information collected and used is accurate, complete and up to date. To assist in this, information provided will need to be true, accurate, current, and complete. Information will need to be provided using VWCCS templates created to collect relevant information.

Volunteers and staff are requested to email VWCCS (info@vwccs.org.au, Attn: General Manager) if their Personal Information is inaccurate or incomplete. Requests will be responded to within 30 days and all reasonable efforts will be made to correct Personal Information subject to VWCCS record retention obligations.

R&ID will do annual update requests relating to personal information to all volunteers.

VICTIMS & WITNESSES
of CRIME COURT SUPPORT

Storage and Security of Volunteer and Staff Personal Information

VWCCS aims to keep Personal Information secure and takes reasonable steps to protect all prospective, current and past Volunteers' and staff Personal Information it holds from misuse, interference, loss and from unauthorised access, modification or disclosure.

These steps include:

- Holding any paper records securely in one location in a locked filing cabinet.
- Accessing Personal Information on a need-to-know basis, by authorised personnel.
- Ensuring our premises have secure access; and ensuring storage and data security systems and protections are regularly audited.
- Deleting information as personal information when volunteers resign.

Any Personal Information held on VWCCS computer systems is stored in secure data storage facilities. Information should be disaggregated where possible to limit access to sensitive information. Records will be checked regularly and updated and/or deleted on an annual basis.

Questions, Problems or Complaint about use of Personal Information

If Volunteers or staff feel that their privacy has not been respected or that VWCCS has conducted itself inconsistently with this VWCCS Privacy Policy, or for any other queries in relation to this VWCCS Privacy Policy, they should contact the VWCCS General Manager.

Any complaints will be investigated and the Volunteer or staff member will be notified of the outcome of the investigation within a reasonable time. Complainants will be advised if the complaint can be resolved quickly or whether more time is required to investigate and resolve the complaint.

Section Two: Client and Referral Agency Information

Three key principles:

- Clients are to be informed of the purpose for collecting any personal information; what will be done with it and who else might access it. Types of information may include the client's name or mobile numbers.
- Personal information collected must be relevant, accurate, up to date and not excessive. The collection of the information should not intrude unnecessarily into the personal affairs of the individual.
- It is important that the client consents to the collection of the information and that the information collected is required for the client to receive the support services provided by VWCCS.

VICTIMS & WITNESSES of CRIME COURT SUPPORT

Collection

- Lawful – when a VWCCS CSO collects a client's personal information, the information must be directly related to VWCCS' activities and necessary for that purpose.
- Direct – VWCCS clients' information must be collected with client's consent.
- Open – the client must be informed that the information is being collected, why it is being collected and who will be storing and using it for adjournments.
- Relevant – VWCCS CSOs must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into the client's personal affairs.
- Confidential – information about clients is not to be shared without specific direction from a court of law, law enforcement agency or authorised regulator.

Storage

- Secure – the client's information must be stored securely, not kept longer than 12 months (or as long as the client's hearing continues) and disposed of appropriately. Paper records should be placed in secure bins and should be protected from unauthorised access, use or disclosure. Information stored electronically should be held securely and deleted after 12 months or at the end of the hearing.

Access

- Transparent – if requested, VWCCS must provide the client with enough details about what personal information they are storing, why they are storing it and what rights the client has to access it.
- Accessible – VWCCS must allow the client to access their personal information without unreasonable delay and expense.
- Correct – VWCCS must allow the client to update, correct or amend their personal information where necessary.

Use

- Accurate – VWCCS must make sure that the client's information is accurate before using it.
- Limited – VWCCS can only use their information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which they have given their consent. It can only be used without the client's consent in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

- Restricted – VWCCS can only disclose clients' information with their consent or if they were advised at the time it was collected from clients that they would do so. VWCCS clients'

information can only be used without their consent to deal with a serious and imminent threat to any person's health or safety.

- Safeguarded – VWCCS cannot disclose clients' sensitive personal information without their consent, for example, information about clients' ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.
- VWCCS can only disclose sensitive relevant information without clients' consent to deal with a serious and imminent threat to any person's health or safety.

Responsibilities for managing privacy

- Responsibilities for the management of personal information about a client are the domain of any individual VWCCS volunteer or staff member within the organisation with access to, or responsibilities for such information.
- VWCCS Management takes responsibility to ensure Volunteers and staff members are suitably instructed on their obligations in relation to the handling and protection of personal information.

Section Three: Data Breach Plan

Purpose

This Privacy Breach Policy outlines the procedures for identifying, responding to, and notifying relevant parties in the event of a data breach involving staff or volunteers at VWCCS. Protecting the integrity and confidentiality of our data is paramount to our mission and the trust of those we serve.

1. Identification of a Breach

When a data breach is identified, it is crucial to act swiftly to mitigate any potential damage. The following steps should be taken:

- **Immediate Notification**: The individual who identifies the breach must notify the General Manager as soon as possible, providing details about the nature and scope of the breach.

2. Notification Protocol

Once a breach has been confirmed, the following parties will be notified and include:

a. Internal Notification

- **Who**: General Manager, HR, and Board.
- **What**: A detailed report of the breach, including the nature of the breach, types of data affected, number of individuals impacted, and any immediate actions taken.
- **When**: Within 24 hours of identifying the breach.

b. External Notification

- **Who**: Affected individuals, relevant regulatory bodies, and law enforcement if necessary.
- **What**: Clear communication detailing the nature of the breach, the types of data involved, potential consequences, and steps being taken to address the breach. Affected individuals will also be informed about measures they can take to protect themselves.
- **When**: Within 72 hours of confirming the breach, as required by applicable regulations.

3. Investigation and Remediation

Following notification, an internal investigation will be conducted by an appointed committee to determine:

- The cause of the breach
- The extent of the data compromised
- Measures to prevent future breaches

A risk assessment and remediation plan will be implemented, including any necessary changes to our data security practices.

4. Multi-Factor Authentication (MAY NOT REQUIRED/SUITABLE?)

To enhance our data security, all staff and volunteers with access to sensitive data must utilize multi-factor authentication (MFA). This measure requires users to provide two or more verification factors to gain access to our systems, reducing the risk of unauthorized access in the event of stolen passwords or other breaches.

Note: This will be implemented with the rollout of the Intranet in early 2025

5. Training and Awareness

All staff and volunteers will receive regular training on data security practices, including recognizing potential threats and understanding their responsibilities in reporting any data breaches.

6. Review and Update

This policy will be reviewed annually or as needed following a data breach to ensure its effectiveness and compliance with relevant laws and regulations.

Date published: November 2024 Review date: December 2025

Conclusion

By adhering to this Data Breach Plan, VWCCS Inc aims to protect sensitive data and respond effectively in the event of a breach, ensuring the continued trust of our stakeholders and the integrity of our mission.

VICTIMS & WITNESSES of CRIME COURT SUPPORT

Section 4: Consequences for Data Breach

In the event that a staff member or volunteer is found responsible for a data breach due to negligence, malicious intent, or failure to comply with established policies, the following may apply:

1. Investigation

- **Preliminary Assessment**: An initial investigation will be conducted to determine the circumstances surrounding the breach, including whether it was intentional, negligent, or due to a lack of training.
- **Recommendations**: The committee undertaking the investigation will assess the severity of the breach, and recommend actions.

2. Disciplinary Actions

Depending on the findings of the investigation, disciplinary actions may include:

- **Verbal Warning**: For minor infractions or first-time offenses where negligence and no harm is determined.
- **Written Warning**: For repeated infractions or more serious negligence, outlining the behaviour and the consequences of future violations.
- **Mandatory Training**: Requirement to undergo additional training on data security and organisational policies.
- **Suspension**: Temporary removal from duties, particularly for serious breaches or repeated offenses.
- **Termination**: Immediate termination of employment or volunteer status for severe breaches, especially those involving intentional misconduct, gross negligence, or a breach of trust.

3. Legal Consequences

If the breach results in legal violations or damages to individuals or the organisation, the responsible individual may face legal action, which could include:

- **Civil Liability**: Financial penalties or restitution claims from affected parties.
- **Criminal Charges**: In cases of intentional wrongdoing or severe negligence, criminal charges may be pursued.

4. Reputational Consequences

- The individual may face reputational damage within the organisation and the broader community, impacting future employment or volunteer opportunities.

5. Review of Access Privileges

- A review of the individual's access to sensitive data will be conducted, which may lead to a reassessment of their roles and responsibilities within the organisation.

Conclusion

Consequences for data breaches are crucial for maintaining accountability and ensuring a culture of data security within VWCCS. All staff and volunteers should be aware of these potential consequences to encourage adherence to data protection policies.