Data Privacy & Confidentiality Policy

1. Purpose & Rationale

1.1. This policy describes how DVAC collects, handles and protects personal information. It outlines the types of personal information usually collected, the purposes for which it is collected, to whom DVAC may disclose information, how it is held and kept secure and individual rights in relation to personal information, including how to complain and how DVAC will deal with complaints.

2. Position Statement/Scope

2.1. DVAC takes confidentiality and privacy of information seriously, including the right to remain anonymous if a client chooses. We recognise our duty of care to safeguard information which could jeopardise the security and safety of our employees and the adults, children or young people accessing DVAC services.

2.2. DVAC will handle data in accordance with our internal policies and regulatory obligations, including compliance with the National and Queensland privacy principles and the Privacy Act 1988, Information Privacy Act 2009 (Qld), Right to Information Act 2009 (Qld), and Information Privacy and Other Legislation Amendment Act 2023 (Qld).

2.3. This policy applies to all individuals handling DVAC data, including the Board of Directors, Management team, and all employees of DVAC, as well as, external contractors, volunteers, students and partner agencies. It covers the governance of personal, operational, and case-related data, whether stored physically or digitally.

3. Expected Outcome

3.1. Compliance with documented data consent, access and disclosure controls.

3.2. Reduced incidence of privacy data breach.

3.3. Timely and transparent privacy related complaints handling.

4. Definitions

Term	Definition
Access controls	DVAC data is classified by type and access restrictions are applied based on sensitivity, regulatory requirements, and operational needs. Methods for implementing these restrictions are referred to as access controls. See DVAC's Data Governance Framework (Section 3) for more information.
Confidentiality	Protection of personal and sensitive information from unauthorised access.
Data breach	A data breach occurs when personal information is subjected to unauthorised access or disclosure, or where the information is lost, and unauthorised access or disclosure is likely to occur.

Term	Definition
	Example: data breaches resulting from human error - • Loss of an employee's laptop, USB or paper records that contain personal information held by DVAC (e.g. left on a train, at the airport etc.) • An employee accidentally disclosing personal information to the wrong recipient (e.g. sending correspondence to the wrong employee) Example: data breaches resulting from malicious activity - • Hacking into DVAC's email accounts, software or databases containing Personal Information • Scams that trick an employee of DVAC into releasing personal information • Inappropriate or fraudulent use of a database containing personal information Example: data breaches resulting from unforeseen circumstances – • Unforeseen events that occur to a contractor who holds personal information on behalf of DVAC or if a cloud service provider suffers a data breach (e.g. Microsoft)
Personal information	Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion— (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.
Sensitive information	Sensitive information is a specific category of personal information, and is information or an opinion about an individual's: • racial or ethnic origin • 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 • health information • genetic information that is not otherwise health information

Term	Definition
	• biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.

5. Roles & Responsibilities

Roles	Responsibilities
Board	• Provide strategic oversight of DVAC's privacy and confidentiality practices, ensuring alignment with risk appetite.
CEO	• CEO approve policy and procedure. • Own and manage DVAC's privacy risk profile, including oversight of data breach response and incident escalation. • Ensure privacy and confidentiality controls are embedded in strategic and operational planning and lead compliance. • Report to the Board on privacy risks, incidents, and mitigation strategies. • Ensure staff training and resources are available to support privacy compliance.
People Leaders	• Implement privacy and confidentiality procedures across teams, including access controls and consent management. • Monitor and report privacy risks, breaches, and concerns. • Ensure team members understand and apply privacy principles in daily operations. • Promote a culture of transparency, respect, confidentiality, and ethical data handling.
Employees	• Understand and comply with DVAC policies and procedures. • Handle personal and sensitive information responsibly, including secure storage and sharing. • Obtain and document informed consent where required. • Report suspected breaches or privacy concerns promptly.

6. Privacy Notice

6.1. Privacy notice

6.1.1. Domestic Violence Action Centre Inc (ABN 91 593 855 217) ("DVAC", "we", "our" or "us") may collect your personal information when you interact with us, including when you call us, when you complete our forms, when you contact us with a comment, enquiry or complaint through our website or social media, when you email us and when you otherwise interact with us.

6.1.2. DVAC collects your personal information from you directly and from other sources, such as third parties and publicly available sources, to provide our services, to manage and conduct our business, to offer or promote our services, to obtain feedback, to help us manage, develop and enhance our services, to consider your suitability for employment and to comply with our legal obligations, resolve any disputes and enforce our agreements and rights with third parties.

6.1.3. If you do not provide or DVAC cannot otherwise collect all the information we request or need, DVAC may not be able to provide our services to you.

6.2. Sharing your personal information

6.2.1. We may share your personal information for safety, legal, and/or support planning purposes, including with your consent for your health and wellbeing, to comply with our duty of care, to comply with our legal obligations and/or to comply with our reporting requirements and manage our business.

6.3. Information about our services

6.3.1. With your consent, we may use your contact details to send you (by telephone, post, email or SMS marketing communications about news or events current to DVAC. You can opt out of marketing communications at any time, by following the unsubscribe function in the message we send or emailing us at complaints@dvac.org.au

6.4. Further information

6.4.1. Our privacy policy, which is available at www.dvac.org.au includes our contact details, explains more about the types of personal information we usually collect and how we handle your personal information, as well as how you can seek access to and correction of your personal information, how to make a privacy complaint and how we deal with these complaints.

7. Collection of personal information

7.1. As outlined in our Data Governance Framework, DVAC will collect data on an as needs basis, aligning with the scope of operations and reporting requirements. Data collection must be justified, relevant, and necessary for service delivery, reporting obligations, and operational management.

7.2. The type of personal information collected depends on the operational and service delivery requirements, and may include:

7.2.1. personal details, such as your name, date of birth, postal address, email address, telephone number and details of your guardian (if applicable)

7.2.2. financial details, such as your employment status, occupation and annual income

7.2.3. demographic information, such as age, sex, religion, family type, country of birth, year of arrival in Australia and language spoken at home

7.2.4. medical information

7.2.5. IP address and browser user agent string

7.2.6. any additional information you provide through our forms or website

7.2.7. information about the matter you are seeking assistance with; and, for prospective employees may also include

7.2.8. employment history and qualifications

7.2.9. academic records

7.2.10. references

7.2.11. medical information
7.2.12. personal alternative contact details
7.2.13. superannuation fund details
7.2.14. criminal history record.

7.3. Access to information collected is limited to DVAC employees specific to the purpose of service delivery and operational management.

7.4. If unsolicited (unrequested) personal information is received by DVAC, that could not have been obtained by lawful means, it will be destroyed or de-identified as soon as practicable and in accordance with the law. For more information DVAC's Data Management Policy.

8. Collection of information from individuals

8.1. Information will be collected directly from individuals who may 'opt in' to share personal information collected via telephone calls, emails, DVAC forms, online enquiries, feedback, compliments or complaints.

8.2. Our Rights & Obligations Policy recognises the rights of individuals accessing our services to choose to remain anonymous or use an alias where possible and lawful. This will limit our ability to respond to enquiries and delivery services.

9. Collection of information from third parties

9.1. Information will be collected via third parties with whom we interact in order to provide our services and operations. For more information see DVAC's Data Usage & Sharing Policy.

9.2. DVAC may collect personal information from third parties where consent has been provided, including medical and health providers, government agencies, non-government service providers, guardians or authorised representatives. In these instances, DVAC will take reasonable steps to ensure individuals are aware of the collection and its context.

9.3. DVAC may also collect personal information generated or inferred by AI systems, where direct collection is impracticable or where individuals have given informed consent for AI use. All personal information collected through these methods will be managed in accordance with the Australian Privacy Principles (APPs) and DVAC's policies, ensuring fairness, accuracy, and transparency in AI use—especially where decisions may affect individuals.

9.4. DVAC may collect information on prospective employees from third parties and publicly available sources.

10. Collection of online data

10.1. Data provided via DVAC's website or social media will be collected, including the IP address and browser user agent string to help spam detection. An anonymised string created from an individual's email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service privacy policy is available here. After approval of a comment, an individual's profile picture is visible to the public in the context of their comment.

10.2. Data linked to images uploaded to DVAC's website or social media, will be collected. As such individuals should avoid uploading images with embedded location data (EXIF GPS)

included. Visitors to the website or social media can download and extract any location data from images on the website or social media.

10.3. DVAC may also use 'cookies' or other similar tracking technologies that tracking of website usage and preferences. Cookies are small files that store information on an individual's device. They enable the entity that installed the cookie to recognise a user across different websites, services, devices and/or browsing sessions. Cookies can be disabled internet browser settings which may limit the functionality of the DVAC website for the user.

10.4. Content embedded on the DVAC website (e.g. videos, images, articles, etc.) from other websites behaves in the exact same way as if the visitor has visited the other website. These websites may collect data about, use cookies, embed additional third-party tracking, and monitor interaction with that embedded content, including tracking interaction with the embedded content if an individual has an account and are logged in to that website.

10.5. DVAC uses analytics to understand how DVAC's website and social media are being used, including the demographics of individuals accessing the content provided.

11. Visitor Privacy Collection Notice

11.1. DVAC may request at our discretion for visitors to provide their name and date of birth when attending our offices. This information is used by DVAC to confirm if there is any reason to be concerned about a person's presence at our offices.

11.2. Names and dates of birth in these matters are not disclosed to any third party unless permitted or required by law. Visitor information is held on the Visitor Register held at each DVAC site. The requirement for Visitor detail checks is held on a Privacy Collection Notice displayed in the reception area of each DVAC office.

11.3. If a person declines to provide their name and date of birth they may not be permitted to enter or remain at the DVAC office. A person may be requested to leave if identified as a person of concern and advised they cannot enter DVAC premises due to a conflict of interest.

12. Data Access Management

12.1. DVAC enforces strict access management protocols to protect personal information. Access to data is role-based, meaning only authorised personnel with a defined operational need may access specific types of information, as defined in our Data Governance Framework. All access is logged and monitored to ensure accountability and traceability.

12.2. Individuals may request access to, or correction of, the personal information DVAC holds about them at any time via DVAC's website. DVAC will verify the individual's identity before responding to any request. Subject to applicable exceptions under the *Privacy Act 1988*, DVAC will provide access within a reasonable timeframe, typically within 28 days. If access is refused, DVAC will provide a written explanation and information about external complaint avenues. For more information see the Data Request Response Procedure.

12.3. Any request for access to client information from an external third party must be made in writing and directed to the relevant Team Leader or Manager for approval. Requests must clearly identify the information sought, the purpose of the request, and the legal authority or client consent under which the request is made. DVAC will assess each request in

accordance with our legal obligations for client privacy, safety and duty of care. Where appropriate, DVAC will seek informed consent from the client prior to disclosure. For more information see the Data Usage & Sharing Policy and related procedures.

12.4. All disclosures will be logged, and a record of the decision-making process is retained for audit and review purposes. DVAC will not release client information without lawful authority, valid consent, or a court order.

13. Data Use & Disclosures

13.1. We will only use your personal information for the purposes for which it is given to us, or for the purposes which are related (or directly related in the context of using sensitive information) to one or more of our functions or activities unless required or authorised by law. The collection of sensitive information will be explicitly justified under permitted health situations, legal obligations, or individual consent. We may collect, use and hold information to provide our services; to manage and conduct our business; to offer or promote our services; to obtain feedback; to help us manage, develop and enhance our services, including our websites and applications; to consider suitability for employment; and to comply with our legal obligations, resolve any disputes and enforce our agreements and rights with third parties. For more information on how we use data collected see DVAC's Data Usage & Sharing Policy.

13.2. DVAC will only keep personal information for as long as it is required for the purpose for which it was collected or as otherwise required by applicable laws.

13.3. In some instances, DVAC may use personal information to contact individuals about news or events current to DVAC. Direct marketing about DVAC events and news may be utilised only in the instances where a person provides consent through 'opting in.' DVAC will never use or disclose personal information for direct marketing related purposes without consent. Individuals can withdraw consent to receiving direct marketing communications at any time by unsubscribing from the mailing list using the 'opt out' function, or via DVAC's feedback and complaints process.

13.4. The sharing and disclosure of information by DVAC is usually for safety, legal and/or support planning purposes. DVAC will always aim to obtain consent before disclosing information to third parties. Individuals may consent to the disclosure of certain information and may ask DVAC to share information on their behalf with another person, stakeholder, organisation, or service. In situations of imminent risk, DVAC has a duty of care to act to ensure safety. Legal obligations may require disclosure under child protection laws, subpoenas, or the DFV Protection Act 2012. DVAC also shares de-identified data with funding bodies and may disclose information to contracted service providers, professional advisers, or in the event of business transfer. All disclosures are made with respect for an individual's privacy, and DVAC will involve impacted individuals in decision-making wherever possible and safe, only sharing personal information as permitted by law or with prior consent.

13.5. Consent for the collection, use, and disclosure of personal information must be documented and reviewed regularly. DVAC obtains informed consent at the point of service engagement, and reviews consent when there are changes to service delivery, data sharing arrangements, or the individual's circumstances. Consent may be withdrawn at any time, and DVAC will update records accordingly.

13.6. Concerns about how DVAC's deals with personal information, can be raised via DVAC's feedback and complaints process. All complaints will be reviewed and investigated in accordance with DVAC's Rights & Obligations Policy and Client Feedback & Complaints Procedure.

14. Child Safety

14.1. DVAC is committed to upholding the privacy, safety, and rights of children and young people in all counselling and support services.
14.2. As a Child Safe Organisation, we seek informed consent from parents or legal guardians for children aged 0–17 to engage in counselling or group programs, while also ensuring that children are actively involved in the decision to participate in an age-appropriate manner.
14.3. Information sharing prioritises child safety while respecting privacy through clear protocols about what information is shared, with whom and for what purpose.
14.4. Children and families are informed about information sharing unless this would increase risk or compromise safety or investigations.
14.5. For young people aged 14–17, DVAC recognises that there may be valid reasons for seeking counselling without parental involvement. In such cases, DVAC counsellors will assess the young person's capacity to provide informed consent and ensure that engagement is appropriate, safe, and respectful of their circumstances. Where a young person consents to engage without parental involvement, DVAC will take additional care to ensure their privacy is respected, and any sharing of information will occur only with their informed consent or where required by law (e.g. risk of harm).
14.6. Records management ensures secure storage, restricted access and appropriate retention periods in compliance with legislative requirements.
14.7. All decisions are guided by child safety principles, legal obligations, and DVAC's commitment to privacy and confidentiality. For more information see Confirming Client Consent Procedure and Acting on or Reporting Child Abuse or Neglect Procedure.

15. Data Breach Mitigation

15.1. DVAC is committed to proactively managing data breach risks through robust prevention, detection, and response strategies that uphold the privacy and safety of individuals. As part of this commitment, DVAC enforces practical controls including role-based access restrictions, two-factor authentication, automated device locking, supervision and strict technology use protocols.
15.2. Employees must adhere to the Technology User Agreement and Work From Home Agreement, avoid using USB devices for sensitive data, and ensure all client-identifiable information is securely stored and locked at all times.
15.3. These measures form part of DVAC's broader Risk Management and Data Governance Frameworks. DVAC's Data Breach Response Procedure outlines DVAC's approach to managing suspected data breaches and is compliant with the Office of the Australian Information Commissioner (OAIC) guidance and *Mandatory Breach Notification* requirements under *Qld IP Act (Chapter 3A)*.

16. Related Documents

16.1. External legislation and guidelines include:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Queensland Privacy Principles (QPPs)
- Information Privacy Act 2009 (Qld)
- Right to Information Act 2009 (Qld)
- Information Privacy and Other Legislation Amendment Act 2023 (Qld)
- Office of the Australian Information Commissioner (OAIC) Privacy Guidelines for NFPs

16.2. Internal Resources

- Data Governance Framework
- Data Management Policy
- Data Usage & Sharing Policy
- Cyber Security Policy
- Acceptable Use of Technology Policy
- Governance Policy
- Code of Conduct
- Schedule of Delegations
- Rights & Obligations Policy
- Data Breach Response Procedure
- Client Feedback and Complaints Procedure
- Sharing Information with Third Parties Procedure
- Data Request Response Procedure
- Confirming Client Consent Procedure
- Consent to Release or Obtain Information form

17. Consultation

17.1. The development of this policy involved consultation with key internal stakeholders, including the Combined Leadership Team (CLT), Executive Leadership Team (ELT), and relevant staff subject matter experts including DVAC's IT partners.

18. Owing Team

18.1. The Business Services team is responsible for implementation, review, and continuous improvement of this policy.

19. Review Schedule

19.1. The review cycle for DVAC policy documents: all new policies, as well as existing policies undergoing review or updates, will be formally reviewed every two (2) years. However, earlier reviews may be initiated if there are significant legislative changes, shifts in organisational structure, or emerging sector requirements that impact the relevance or

effectiveness of the policy. This ensures that DVAC's policies remain current, compliant, and aligned with best practice and organisational.

Version	Date Endorsed	Review Date	HSQF Standard	Approved by	Content reviewed/ purpose
1	11/11/2025	1/10/2027	1, 4, 5, 6	CEO	New policy with content adapted from Rights & Obligations Policy v6 and Risk & WHS Policy v4. Reformatted using new policy template.