

VHKA

Privacy Policy



Help for non-English speakers

If you need help to understand this policy, please contact wade.ho@vhka.org.au

Purpose

The purpose of this policy is to outline how VHKA manages and protects a participant's personal information to ensure compliance with all Commonwealth and Victorian privacy legislation and the NDIS Act 2013.

Types of Information

The type of information VHKA collects and holds includes (but is not limited to) personal information, including sensitive information, about:

- Participants before, during and after the course of their participation in VHKA's organised events and activities;
- Job applicants, staff members, volunteers and contractors; and
- Other people who come into contact with VHKA.

Personal Information You Provide

VHKA will generally collect personal information about an individual by way of forms filled out by participants, face-to-face meetings and interviews, and telephone calls.

Personal Information Provided by Other People

In some circumstances VHKA may be provided with personal information about an individual from a third party; for example a report provided by a medical professional.

Exception in Relation to Employee Records

Under the Privacy Act the National Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to VHKA's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between VHKA and employee.

Use of Information

VHKA will use personal information it collects for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and are reasonably expected, or to which individuals have consented.

Children and Parents

In relation to personal information of children and parents, VHKA's primary purpose of collection is to enable VHKA to provide services for children and parents. The purposes for which VHKA uses personal information of children and parents include:

- Day to day administration;
- Looking after children's social and medical wellbeing while receiving VHKA's services;
- Seeking donations and marketing for VHKA; and
- Satisfying VHKA's legal obligations and allowing VHKA to discharge its duty of care.

In some cases where VHKA requests personal information about a child or parent, if the information requested is not obtained, VHKA may not be able to provide services to them.

Job Applicants, Members of Staff and Contractors

In relation to personal information of job applicants, staff members and contractors, VHKA's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

The purposes for which VHKA uses personal information of job applicants, staff members and contractors include:

- Administering the individual's employment or contract, as the case may be;
- For insurance purposes;
- Seeking funds and marketing for VHKA; and
- To satisfy VHKA's legal obligations, for example, in relation to child protection legislation and child safety standards.

Volunteers

VHKA obtains personal information about volunteers who assist VHKA in its functions, to enable VHKA and the volunteers to work together, to satisfy VHKA's legal obligations, including compliance with child protection legislation and child safe standards.

Marketing and Fundraising

VHKA treats marketing and seeking donations for the future growth and development of VHKA as an important part of ensuring that VHKA continues to be a quality service provider.

Personal information which is not sensitive information held by VHKA may be disclosed to an organisation that assists in VHKA's fundraising.

Staff, volunteers, contractors and other members of VHKA may from time to time receive fundraising information like newsletters and magazines, which include personal information, may be used for marketing purposes.

If an individual does not wish personal information to be disclosed for these purposes, they may contact the Committee to make the necessary arrangements for the non-disclosure.

Disclosure of Personal Information

VHKA may disclose personal information, including sensitive information, held about an individual to:

- Government departments, if required by law;
- Medical practitioners;
- People providing services to VHKA;
- Debt collection agencies; and
- Anyone VHKA has been authorised to disclose information to.

Sending Information Overseas

VHKA will not send personal information about an individual outside Australia without:

- Obtaining the consent of the individual (in some cases this consent will be implied); or
- Otherwise complying with the Australian Privacy Principles.

Treatment of Sensitive Information

In referring to 'sensitive information', VHKA means information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information; and health information about an individual. Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and Security of Personal Information

VHKA's staff members are required to respect the confidentiality of personal information and the privacy of individuals.

VHKA has in place steps to protect the personal information VHKA holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass-worded access rights to computerised records.

Updating Personal Information

VHKA endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by VHKA by contacting the Committee at any time. The Australian Privacy Principles require VHKA not to store personal information longer than necessary.

Right to Access Personal Information

Under the Commonwealth Privacy Act, an individual has the right to obtain access to any personal information which VHKA holds about them and to advise VHKA of any perceived inaccuracy. There are some exceptions to this right set out in the Act.

To make a request to access any information VHKA holds about you or your child, please contact the Committee in writing. VHKA may require you to verify your identity and specify what information you require.

VHKA may charge a fee to cover the cost of verifying your request and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, VHKA will advise the likely cost in advance.

Consent and Rights of Access to Information Regarding Children

VHKA will treat consent given by parents as consent given on behalf of the child, and notice to parents will act as notice given to the children.

Parents may seek access to personal information held by VHKA about them or their child by contacting the Committee. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on

the privacy of others, or where the release may result in a breach of VHKA's duty of care to the children.

Medical Information

Medical information of VHKA staff is covered by the Health Records Act and the Health Privacy Principles. This section of the policy extends to health information collected by VHKA about staff as well as children and other individuals and may include:

- Emergency contacts, next of kin;
- Names of doctors, dentists and other health professionals;
- Assessments, referrals, correspondence with parents;
- Health fund details, ambulance subscription and Medicare number;
- Medical background (including conditions, treatments etc.);
- Immunisations;
- Nutrition, dietary requirements; and
- Diagnosis of disorders, learning difficulties.

Medical information is only collected from individuals, or where the individual is a child, from or with the consent of parents/guardians. This information is collected:

- In order to provide a health service. This includes activities to assess, maintain or improve the individual's health, for diagnosis or treatment or dispensing prescription drugs (as prescribed by a registered practitioner);
- To assess a child's, an employee's, or another individual's ability to participate in certain activities; and
- To assess an employee's fitness to return to work after serious illness or injury.

Enquiries

If you would like further information about the way VHKA manages the personal information it holds, please contact the Committee. Any complaints in relation to VHKA's privacy management will be handled as per VHKA's Complaints Policy.

Serious Harm

The Explanatory Memorandum to the Act explains that serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in VHKA's position would identify as a possible outcome of the data breach.

The Explanatory Memorandum also emphasises that though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not in itself be sufficient to require notification unless a reasonable person in VHKA's position would consider that the likely consequences for those individuals would constitute serious harm.

It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of "serious harm" that may give rise to the notification.

What Happens When There Has Been a Notifiable Data Breach?

Where an eligible data breach is suspected or believed to have occurred, VHKA:

- Carries out a risk assessment in the event that an eligible data breach is suspected;

- Prepares a statement of prescribed information regarding an eligible data breach that is believed to have occurred;
- Submits the statement to the OAIC;
- Contacts all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

Each of these steps is explained in more detail below.

Suspected Eligible Data Breach

If VHKA suspects an eligible data breach may have occurred it must conduct a risk assessment which involves:

- Assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances;
- Taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

VHKA may undertake a risk assessment where an individual has made a complaint in relation to the security of personal information and VHKA suspects that an eligible data breach may have occurred, but further information is required to ensure the criteria of an eligible data breach is met.

If the risk assessment reveals that an eligible data breach has occurred, VHKA then follows the notification requirements under the Act and notifies both the OAIC and if practicable, the individual/s affected.

Notifying the OAIC

Once VHKA has reasonable grounds to believe that there has been an eligible data breach, VHKA:

- prepares a Statement in the prescribed format
- gives a copy of the Statement to the OAIC as soon as practicable after VHKA becomes aware of the eligible data breach.

The Statement sets out:

- the identity and contact details of VHKA;
- a description of the eligible data breach that VHKA has reasonable grounds to believe has happened;
- the kind/s of information concerned;
- Recommendations about the steps that individuals should take in response to the eligible data breach that VHKA has reasonable grounds to believe have happened.

If VHKA believes that another entity regulated by the Act is involved in the eligible data breach, the Statement must include information about the other entities.

Notifying the Individual/s

As soon as practicable after notifying the OAIC, VHKA notifies each of the individuals to whom the relevant information relates or notifies each of the individuals who are at risk from the eligible data breach. In each case, VHKA take such steps as are reasonable in the circumstances to notify the individuals. What is practicable will involve considerations about the time, effort or cost of a notification. VHKA will also publish a statement on its website; and take reasonable steps to publicise the contents of the Statement it prepared for the OAIC.

Complaints handling and Australian Privacy Principles (APP) breaches

The APPs require VHKA to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to VHKA's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs. VHKA advises individuals in our Privacy Policy of how they may complain about a breach of the APPs and how VHKA will deal with that complaint. A copy of VHKA's Privacy Policy can be found on VHKA's website.

Consent and young people

The Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy. However, the APPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from children.

In relation to consent and young people, the APP Guidelines provide as follows:

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise.

An individual aged under 15 is presumed not to have capacity to consent.

The Australian Law Reform Commission (ALRC) also considered the issue of consents by children and young people and recommended that the Privacy Act should be amended to provide that where an assessment of capacity to provide consent 'is not reasonable or practicable' an individual of the age of 15 or over should be capable of giving consent and a person under that age should be presumed not to be capable of giving consent.

The ALRC also noted that people with parental responsibility had some authority to make decisions on behalf of their children who lacked capacity if it was part of a duty to provide for their welfare but did not suggest that such authority extended to all situations.

A parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States and Territories the age of majority is 18 years.

For these reasons, one approach would be for VHKA to adopt the view that in many circumstances, the contract with the parents will govern their relationship with the child in relation to privacy, and thus consents given by parents will act as consents given on behalf of the child and notice to parents will act as a notice given to the child.

However, this approach will not be appropriate in all circumstances. VHKA should recognise that young people do have rights under the Privacy Act and in some circumstances it would be appropriate to seek consents from them, particularly when they are aged 15 or over, as indicated

by the APP Guidelines and ALRC. No doubt in most cases decisions whether to seek information or consents from children or from parents is likely to follow current practices.

Particular issues may arise in the context of information provided to staff members, including counsellors, by children 'in confidence' that is, where the children has asked or expected the staff member not to disclose it. One factor when considering how to deal with such situations will be the age and capacity of the children to provide or refuse consent.

Accountability and responsibilities

Who	Responsibilities
Chairman / Vice-Chairman	Ensure that privacy of our participants is a priority for VHKA
Secretary	-Establish an effective, professional confidential information handling system -Ensure that VHKA staff are aware of the policies and procedures related to privacy
Committee member	-Manage the confidential information handling function -Receive and manage information that is highly sensitive and confidential -Review the Privacy Policy every 2 years
Staff/employees	- Comply with VHKA Privacy Policy - Treat all confidential information of participants with reasonable care and diligence - Comply with escalation protocols, where required

Related policies and further information

- Child Safety and Wellbeing Policy
- Child Safety Reporting Obligations Policy and Procedures
- Child Safe Risk Management
- Child Safety Code of Conduct
- Complaints Policy
- Staff and Volunteers Policy

Approval and review

Created date	12 August 2022
Endorsed by	VHKA's committee
Endorsed on	14 August 2022
Next review date	14 August 2022