[HIGHETT RSL SUB-BRANCH Inc]

Privacy Policy *incorporating* Notifiable Data Breach Scheme

Policy

- [HIGHETT RSL SUB-BRANCH Inc] is committed to respecting the privacy of all personal information in its possession.
- These Policy and Procedures also apply to any contracted agencies that are not already covered by the provisions of the Privacy Act 1988 (Cth) ("the Privacy Act").
- As a large organisation that deals with welfare support for members of the ex-service community, [HIGHETT RSL SUB-BRANCH Inc] complies with the relevant sections of the Privacy Act in particular the thirteen Australian Privacy Principles (APPs) that establish the benchmark for how personal information will be handled. These are:

    1. Open and transparent management of personal information
    2. Anonymity and pseudonymity
    3. Collection of solicited personal information
    4. Dealing with unsolicited personal information
    5. Notification of the collection of personal information
    6. Use or disclosure of personal information
    7. Direct Marketing
    8. Cross-border disclosure of personal information
    9. Adoption, use or disclosure of government related identifiers
    10. Quality of personal information
    11. Security of personal information
    12. Access to personal information
    13. Correction of personal information

- These principles form part of [HIGHETT RSL SUB-BRANCH Inc] standard operating procedures, i.e.:
    - [HIGHETT RSL SUB-BRANCH Inc] only collects personal information that is necessary for the functions of the organisation
    - All personal information is only collected by lawful and fair means
    - All personal information that is collected is dealt with in a uniform manner and the highest regard is taken for maintaining its security at all times.
- [HIGHETT RSL SUB-BRANCH Inc] does not use data hosting facilities or enter into contractual arrangements with overseas third party service providers which involve the disclosure of your information to overseas recipients.

- [HIGHETT RSL SUB-BRANCH Inc] may change this policy from time to time. Any updates to this Privacy Policy will be available on the HIGHETT RSL SUB-BRANCH Inc] website. A copy of this policy can be obtained upon request to the Privacy Officer.
- Complaints or concerns regarding breaches of [HIGHETT RSL SUB-BRANCH Inc] privacy and confidentiality policy and procedures will be fully investigated and actioned appropriately.
    - Please contact our Privacy Officer at:
        - Privacy Officer Gavin Williams
        - gavinw@highettrsl.com.au
        - Phone 95321357

        [HIGHETT RSL SUB-BRANCH Inc] , 1 Station Street Highett 3190. Phone 953201357

Responsibilities

Sub-Branch Manager – for ensuring that policy, procedures and other related documents are up to date and for responding to complaints and concerns.

RSL Privacy Officer – for providing information and support across the organisation regarding these policy and procedures and for receiving and investigating complaints and concerns.

Staff, Office Bearers, Pensions & Welfare Officers and Volunteers – for compliance with policy and procedures and reporting areas of concern.

Types of Personal Information Collected.

- ***Information regarding RSL membership***
    - [HIGHETT RSL SUB-BRANCH Inc] maintains a database of information supplied by members on application for membership and updated from time to time. Access to this database is limited to the 'primary purpose' of maintaining membership of the RSL and the forwarding of regular information to members.
- ***Information regarding staff***
    - [HIGHETT RSL SUB-BRANCH Inc] maintains relevant personal details and other information required in relation to recruitment and ongoing employment of staff. Access and use of this information is limited to 'primary purpose'.
- ***Information regarding volunteers***
    - HIGHETT RSL SUB-BRANCH Inc] maintains relevant personal details and other information required in relation to recruitment and ongoing management of volunteers. Access and use of this information is limited to 'primary purpose'.

- ***Information regarding Day Club participants***
    - [HIGHETT RSL SUB-BRANCH Inc] holds information about Day Club participants, including date of birth, next of kin and other information that is relevant and important in ensuring the safety and wellbeing of participants while they are involved with Day Club activities.
    - The main purpose for which [HIGHETT RSL SUB-BRANCH Inc] holds this information is to facilitate safety and enjoyment while attending Day Club activities, and to enable the most appropriate course of action in the event of an emergency.
    - All Day Club volunteers receive information and training in privacy and confidentiality as part their induction program.
    - On enrolment, Day Club participants are advised about the use ('primary purpose') of personal information collected and how this information is stored.
    - Should a situation arise whereby the disclosure of this information would be to achieve a 'secondary purpose' such as a research project, written permission will be obtained from the Day Club participant beforehand.
- ***Information regarding Welfare Clients***
    - [HIGHETT RSL SUB-BRANCH Inc] holds information about pensions and welfare clients, including date of birth, next of kin, service details, relevant medical records and financial information. Some of this information is considered 'Sensitive Information'
    - The main purpose for which [HIGHETT RSL SUB-BRANCH Inc] holds this information is to process and support clients' claims for pensions and other benefits, to make referrals to services such as health, aged care and crisis support, and to provide RSL welfare and aged care support activities such as friendly visiting, transport to appointments, bereavement support, participation in social / recreational / commemoration activities etc.
    - [HIGHETT RSL SUB-BRANCH Inc] may disclose some of this information to the Department of Veterans' Affairs, health services or other human services agencies in order to achieve the 'primary purposes' in relation to its advocacy, welfare and aged care support functions.
    - As far as possible all welfare clients are given a Privacy of Personal Information Policy Statement that outlines [HIGHETT RSL SUB-BRANCH Inc] policy and responsibilities regarding the use and storage of personal information that is collected.
    - Should a situation arise whereby the disclosure of this information would be to achieve a 'secondary purpose' such as a research project, written permission will be obtained from the welfare client beforehand. A welfare client's decision not to permit release of information for a 'secondary

purpose' will be respected unless there is a lawful reason as to why disclosure of such information is deemed to be necessary. For example, to prevent serious harm or to facilitate legal requirements.

Training for Staff, Welfare Officers and Volunteers

- New staff, office bearers, welfare and pensions officers and volunteers are required to sign Privacy & Confidentiality Agreement Forms.
- [HIGHETT RSL SUB-BRANCH Inc] policies and procedures regarding privacy and confidentiality are explained to new staff, office bearers, welfare and pensions officers and volunteers as part of orientation to their new role.
- Responsibilities for privacy and confidentiality are included in staff and volunteer handbooks. As appropriate, responsibilities are reinforced in meetings and ongoing training.

Procedures relating to the Australian Privacy Principles (APPs)

The following procedures provide an overview of the APPs. Further guidance should be obtained from the [HIGHETT RSL SUB-BRANCH Inc] Privacy Officer where uncertainty exists about the collection, storage or disclosure of personal information.

- ***Collection***
    - [HIGHETT RSL SUB-BRANCH Inc] only collects personal information that is directly necessary for the efficient conduct of its core activities.
    - Information is only collected with the knowledge and consent of the persons concerned.
    - [HIGHETT RSL SUB-BRANCH Inc] provides information to members, staff, volunteers and clients regarding the type of personal information it collects and the way(s) that personal information may be used.
    - Individuals are advised of the consequences (if any) if all or part of the information is not provided.
    - As far as possible all new members and clients are given a copy of the Privacy of Personal Information Policy Statement.
    - Individuals and/or their nominated representative(s) may access their personal information via a Request to Access to Confidential Information form.
- ***Use and disclosure***
    - [HIGHETT RSL SUB-BRANCH Inc] uses personal information about individuals to enable the organisation to fulfil its mission and thereby conduct core business:
        - Information about staff and volunteers is used to support day-to-day operations and management of services and other activities.

        - Information about members is required to manage the membership of the RSL.
        - Information about Day Club participants is required to facilitate safety and enjoyment while attending Day Club activities, also to enable the most appropriate course of action in the event of an emergency.
        - Information about welfare clients is required to process and support clients' claims for pensions and other benefits; to make referrals to services such as health care, aged care, crisis support etc, and to provide other RSL welfare and aged care support activities such as friendly visiting, transport to appointments, bereavement support, participation in social / recreational / commemoration activities etc.
    - [HIGHETT RSL SUB-BRANCH Inc] may disclose information about welfare clients to the Department of Veterans' Affairs or other human services agencies in order to achieve the 'primary purposes' in relation to its advocacy, welfare and aged care support functions.
    - Should a situation arise whereby the disclosure of information would be in order to achieve a 'secondary purpose' such as a research project
    - HIGHETT RSL SUB-BRANCH Inc] will seek written consent from the person(s) concerned.
    - Decisions not to consent to the release of information for 'secondary purposes' will be respected unless there is a lawful reason as to why disclosure of such information is deemed to be necessary. For example, to prevent serious harm or to facilitate legal requirements.

- ***Data quality***
    - [HIGHETT RSL SUB-BRANCH Inc] takes all reasonable steps to ensure that personal information is kept accurate, up-to-date and complete.
    - Staff, membership and volunteer records are regularly updated and information regarding clients is regularly reviewed.

- ***Data security***
    - Access to personal information is restricted to staff and volunteers who require such information in order to efficiently perform their duties and responsibilities within the organisation.
    - RSL Sub-Branches are not permitted to display personal information in public areas; this includes the names of members and other welfare clients who are unwell or on a 'list' for a Home & Hospital visitor.
    - However, a 'sick board' is permitted where consent from the individual has been given prior to disclosing the personal information. Consent may be given orally or in writing. Where consent is given, a record should be kept of who gave the consent, how and when they gave consent and who obtained the consent.

- Because many individuals within the 'RSL community' are well known to each other there is a high potential for unintentional breach of privacy. Therefore all staff and volunteers who have access to 'sensitive information' are required to exercise extreme caution in social situations and other gatherings where the names of individuals may arise.
- [HIGHETT RSL SUB-BRANCH Inc] takes reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.
- Access to personal information is limited by physical measures (i.e. restricted physical access) and electronic security measures (i.e. electronic passwords).
- Information that is out of date or about former members, staff, volunteers and clients is destroyed by shredding or via a contracted confidential disposal company.

- ***Openness***
  - [HIGHETT RSL SUB-BRANCH Inc] provides information to individuals regarding the types of personal information it collects and the way(s) that personal information may be used.
  - As far as possible all new members and clients are given a copy of the Privacy of Personal Information Policy Statement.

- ***Access and correction***
  - Individuals and/or their nominated representative(s) may access their personal information via a Request to Access to Confidential Information form.
  - All requests must be submitted to the Privacy Officer.
  - Within 45 days after receiving an application, [HIGHETT RSL SUB-BRANCH Inc] will provide the applicant with a written reason for refusal of access to information; or written advice that confirms access to information.
  - Access may be refused where the information could:
    - Pose serious threat to the life or health of the individual;
    - Have an unreasonable impact on the privacy of others;
    - The request is frivolous or vexatious;
    - Be unlawful or likely to prejudice any legal proceedings.
    - Attract legal professional privilege;
    - Reveal the intentions of [HIGHETT RSL SUB-BRANCH Inc] in such a way as to prejudice it in negotiations between it and the individual; or
    - Where an enforcement body requests non-disclosure for reasons of national security.
  - Where information is found to be inaccurate, incomplete, misleading or out-of-date, [HIGHETT RSL SUB-BRANCH Inc] will take steps to correct the information in a timely manner.

- ***Anonymity***
    - [HIGHETT RSL SUB-BRANCH Inc] needs to collect and disclose identifiable information about individuals to enable efficiency of business operations and maximise outcomes for welfare clients.
    - Wherever lawful and practicable however, individuals are given the option of not identifying themselves, for example statistics and surveys.
    - Information may be used for the following purposes but only after identifying features are removed:
        - Reports;
        - Auditing and research;
        - Teaching.
- ***Transfer of information***
    - Apart from the 'primary purpose' transfer of information,
    - [HIGHETT RSL SUB-BRANCH Inc] will only transfer information about an individual with consent of the individual.
    - Where there may be a lawful case for an exception to this, the request must be referred to the Privacy Officer for consideration and action.
- ***Sensitive information***
    - [HIGHETT RSL SUB-BRANCH Inc]] collects information about pensions and welfare clients, including date of birth, next of kin, service details, relevant medical records, current physical and mental health status, family and social status, and financial information. Some of this information is considered 'Sensitive Information'
    - The main purpose for which [HIGHETT RSL SUB-BRANCH Inc]] requires this information is to process and support clients' claims for pensions and other benefits, to make referrals services such as health, aged care, crisis support etc and to provide RSL welfare and aged care support activities such as friendly visiting, transport to appointments, bereavement support, participation in social / recreational / commemoration activities etc.
    - As far as possible this information is collected directly from the person concerned and not disclosed without his / her consent unless lawful circumstances exist. For example, to prevent or lessen an immediate threat to the safety and wellbeing of the person or another party.

Notifiable Data Breach Scheme (NDB)

Background

The Privacy Act requires certain entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

The requirements of the NDB scheme are contained in Part IIIC of the Privacy Act and apply to breaches that occur on or after 22 February 2018.

Key Points

Entities that have existing obligations under the Privacy Act to secure personal information must comply with the NDB scheme.

This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than AU$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.

Entities that have security obligations pursuant to the Privacy Act in relation to particular types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

The Notifiable Data Breaches (NDB) scheme

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Privacy Commissioner of certain data breaches.

The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across industries.

What is a data breach?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

Consequences of a data breach

Data breaches can cause significant harm in multiple ways.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

Business Practices to prevent Data Breaches

HIGHETT RSL SUB-BRANCH Inc]] has business practice standards to reduce the risk of a data breach. These practices are contained within the "Privacy Policy Business Practices" document available for staff, office bearers, welfare and pensions officers and volunteers.