Appendix 1.

Privacy Policy *incorporating* Notifiable Data Breach Scheme

Wangaratta RSL Sub-Branch Business Practices to prevent Data Breaches

Wangaratta RSL Sub-Branch is committed to respecting the privacy of all personal information in its possession. All Staff, Office Bearers, Pensions & Welfare Officers and Volunteers are responsible for compliance with the Privacy Policy and procedures and reporting areas of concern. The RSL Privacy Officer is responsible for providing information and support across the organisation regarding these policy and procedures and for receiving and investigating complaints and concerns.

All Staff, Office Bearers, Pensions & Welfare Officers and Volunteers must read and acknowledge the Wangaratta RSL Sub-Branch ***"Privacy Policy incorporating Notifiable Data Breach Scheme"*** document that accompanies this Business Practices document.

The Notifiable Date Breach Scheme (NDB) only applies to data breaches involving personal information that are likely to result in serious harm to an individual affected. 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. Personal information may include credit card information, medical information, home address, telephone number, email address and bank account details.

Wangaratta RSL Sub-Branch has business practice standards to reduce the risk of a data breach and these practices will be updated and changed from time to time.

Staff, Office Bearers, Pensions & Welfare Officers and Volunteers

- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers should avoid communicating personal information. Communication includes via mail, fax, SMS or email.
- When sending personal data (such as memberships lists) via email, efforts should be made to authenticate the source of the request. Whereby, the data recipient should be a member of the Sub-Branch Committee or authorised representative.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers should avoid printing personal information. If printing, ensure paper is not left lying around. Once finished with the paperwork, the paperwork should be disposed of. Correct methods of disposal include shredding or destroyed via a secure document disposal bin.
- If high risk information such as payroll details, credit card details, medical records or bank account information is required to be held onsite then it should be held in a secure locked location.
- Credit card details should not be recorded formally or informally. For example, formal method may include documents sent to individuals or businesses whereby credit card information is required to be completed on the document and sent back to State

Branch. Informally may include obtaining the credit card information over the phone and writing this down on a piece of paper to then process a payment. Only electronic facilities (i.e. direct bank interfaces) should be utilised in these circumstances.

- When Staff, Office Bearers, Pensions & Welfare Officers and Volunteers are emailing multiple recipients from outside the organisation, the Bcc: function of email should be utilised. This will avoid email addresses from being obtained by persons outside the organisation.
- An appropriate privacy disclaimer is to be included at the bottom of every Staff, Office Bearers, Pensions & Welfare Officers and Volunteers email signature.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers must use complex passwords that are at least eight characters in length and include upper case, lower case, symbol and a number.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers should avoid connecting removable media (i.e. USB Flash Drives, portable devices, etc.) to any hardware that has access to the Wangaratta RSL Sub-Branch network. If the connection of removable media is necessary, the removable media must be BitLocker encrypted. For assistance with this service contact the General Manager.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers should avoid opening and forwarding any suspicious emails or attachments. If in any doubt of a breach, turn off your computer immediately and contact the General Manager.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers must take every precaution to ensure that data is not sent to unauthorised third parties.
- Staff, Office Bearers, Pensions & Welfare Officers and Volunteers must exercise control of external devices accessing the Wangaratta RSL Sub-Branch corporate network. For example, connecting external third-party devices into the network in locations such as meeting rooms.

Information Technology & Systems

- Wangaratta RSL Sub-Branch data will include daily backups to varied media onsite and BitLocker encrypted media offsite.
- All systems should have personalised (not generic) user names and passwords.
- Wangaratta RSL Sub-Branch will maintain up-to-date anti-virus software and email security using best practice industry standards.

General

- The Wangaratta RSL Sub-Branch Privacy Policy will be located on the Wangaratta RSL Sub-Branch website (www.wangarattarsl.org.au).
- If a data breach has occurred or there is suspicion of a data breach occurring then Staff, Office Bearers, Pensions & Welfare Officers and Volunteers need to contact the General Manager immediately.
- The General Manager will maintain a register of any reported privacy breaches and follow the decision-making flow chart listed below.

Appendix 1.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.