**VKS-737 & HF-Tel**
Divisions of the Australian National 4WD Radio Network Inc.
Established 1993 ABN 92 486 729 762
**PO Box 2101** **www.vks737.radio** Telephone: **(08) 7325 2600**
**Elizabeth Park. SA. 5113** email: info@vks737.on.net

POLICY STATEMENT

# Privacy Code of Practice

## 1. Introduction.

1.1 The VKS-737 Radio Network Privacy Code of Practice outlines the obligations of Australian National 4WD Radio Network Inc. and the VKS-737 Radio Network (hereafter referred to as "the Network") under the Privacy Act regarding the collection, use, storage and disclosure of personal information of Network subscribers and patrons and also provides procedures that the Network will follow when collecting, using, storing and disclosing such information.

1.2 The Privacy Code of Practice does not include its own complaints handling mechanism and all complaints are to be handled as set out in the Privacy Act. However, in most instances the Privacy Commissioner would consider it appropriate for the complainant to deal initially with the Network.

1.3 The Privacy Code of Practice outlines guidelines that the Network will follow to ensure a consistent, fair, visible, accessible, responsive and accountable approach to privacy.

1.4 In all instances where a subscriber or individual has made a complaint in respect of their privacy to the Network, the Network will use all reasonable endeavours to ensure that it maintains principles of procedural fairness and uphold obligations of confidentiality as required under the Privacy Act.

## 2. Legislative Requirements

This Privacy Code of Practice is based on the **National Privacy Principles** in the **Privacy Amendment (Private Sector) Act 2000** (Act No. 155 of 2000), and the **Privacy Act 1998** (Act No. 119 of 1998) that was prepared on 10th January 2001.

2.1 The Privacy Act defines organisations as follows:

- businesses, including **not-for-profit organisations** such as **charitable organisations**, sports clubs and unions, with a turnover of more than $3 million;
- federal government contractors;
- health service providers that hold health information (even if their turnover is less than $3 million);
- organisations that carry on a business that collects or discloses personal information for a benefit, service, or advantage (even if their turnover is less than $3 million);
- small business with a turnover of less than $3 million that choose to opt-in;
- incorporated State Government business enterprises; and
- any organisation that regulations says is covered

2.2 The Privacy Act defines annual turnover as follows:

- The annual turnover of a business for a financial year is the total of the following that is earned in the year in the course of the business:
- the proceeds of sales of goods and/or services;
- commission income;
- repair and service income;
- rent, leasing and hiring income;
- government bounties and subsidies;
- interests, royalties and dividends;
- other operating income

2.3 The Privacy Act establishes minimum requirements (known as the National Privacy Principles) in relation to how private organisations should collect, use, keep secure and disclose personal, health and sensitive information that can be recorded in some form (including an electronic record). Additional privacy requirements apply to the public sector, known as the Information Privacy Principles that are not applicable to the Network.

2.4 The Privacy Act defines personal, health and sensitive information as follows:

**personal information** means:

- information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

**health information** means: information or an opinion about:

- the health or a disability (at any time) of an individual; or
- an individual's expressed wishes about the future provision of health services to him or her; or
- a health service provided, or to be provided, to an individual;
- that is also personal information; or
- other personal information collected to provide, or in providing a health service; or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs of body substances.

**sensitive information** means: information or an opinion about an individual's

- racial or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record;
- that is also personal information; or
- health information about an individual

2.5 The Privacy Act requires affected organisations to comply with the National Privacy Principles, as minimum privacy standards. The National Privacy Principles operate as default principles, unless replaced by a Privacy Code of Practice, which must be drafted in accordance with the Privacy Act, the prescribed standards and other guidelines issued by the Privacy Commissioner, including a demonstration of the Privacy Code of Practice as having obligations at least equivalent to the National Privacy Principles.

## 3. Definitions

**"Administration Manager"** means the Administration Manager employed by the VKS-737 Radio Network.

**"Australian National 4WD Radio Network Inc."** means the Australian National 4WD Radio Network Inc. a Prescribed Association registered in accordance with the Associations Incorporations Act (SA) 1985 with the Office of Business and Consumer Affairs in the State of South Australia, and a Public Benevolent Institution and Charity registered with the Australian Taxation Office.

**"Committee Member"** means a Committee Member of the Australian National 4WD Radio Network Inc.

"**contractor**" means independent contractors providing services for the Australian National 4WD Radio Network Inc. and/or the VKS-737 Radio network. These contractors may include but are not limited to individuals, sole proprietors, partnerships, registered businesses, companies, corporations, organisations and charities.

"**direct marketing**" means any approaches made or activities undertaken that promote, advertise or market products or services;

**"employment"** means the act of being employed by the Australian National 4WD Radio Network Inc. or the VKS-737 Radio Network as an employee:

"**Enforcement Body**" means any agency, body, authority, police force or service, of the Commonwealth, a State or Territory which (among other things) is responsible for administering or performing a function under a law that:

- Administers the use of Radiocommunication services within the Commonwealth of Australia.
- Administers the use of Telecommunications services within the Commonwealth of Australia.
- Provides emergency assistance to individuals or organisations.
- Administers the coordinating of emergency service assistance to individuals or organisations.
- Administers the conducting of criminal investigations or inquiries, or the protection of the public revenue.
- Administers the collection of taxation within the Commonwealth of Australia.
- Administers regulations relating to the operation of businesses, companies and associations either within the Commonwealth of Australia or within individual States of Australia or Territories.

**"ex-officio"** means a position of responsibility within an organisation, or representing an organisation, but not an official management or committee position. Examples include, but are not limited to Base Station Operators, Regional Representatives and Show Volunteers.

"**individual**" means any member of the public who has contacted or been in contact with the Network.

**"Network"** means the Australian National 4WD Radio Network Inc. and/or the VKS-737 Radio Network.

**"Operator"** means an employee employed in the role of operating a VKS-737 Base Station, either directly at the site of a Base Station, or remotely via a radio-telephone interconnect.

**"Public Officer"** means the Secretary / **Public Officer** of the Australian National 4WD Radio Officer Inc. a position as defined in the Associations Incorporations Act (SA) 1985.

"**primary purpose**" means the sole, dominant or fundamental reason or purpose for collecting information;

"**Privacy Commissioner**" means the Federal Privacy Commissioner;

"**reciprocal club / organisation**" means a club / organisation that has a reciprocal arrangement with the Australian National 4WD Radio Network Inc and/or the VKS-737 Radio Network.

"**related body corporate**" means:

- a holding company of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate.

"**secondary purpose**" means any reason or purpose other than a primary purpose; and

"**special circumstances**" means only those circumstances associated with preventing a threat to the life of an individual or reducing possible harm or injury to an individual where the individual to whom the information relates is incapable or unable (either by law, a physical limitation or otherwise) to provide consent to the collection of information.

**"sub-contractor"** means an individual or a business that signs a contract to perform part or all of the obligations of another's contract.

"**subscriber**" means any individual who is a current financial subscriber of the Network.

**"VKS-737 Radio Network"** means the VKS-737 Radio Network, a business registered with Office of Business and Consumer Affairs in the State of South Australia.

**"volunteer"** means a subscriber or individual who serves the Network but does not receive payment or receive compensation for the services rendered, however they may be compensated for costs incurred as a result of providing these services.

## 4. Aims

4.1 The aims of this Privacy Code of Practice are to set standards by:

- ensuring compliance of the Privacy Act, including meeting or exceeding the standards stipulated by the National Privacy Principles; and
- creating a culture of confidence and security in the services provided by the Network that involve collection, use, storage and disclosure of personal information; and
- demonstrating commitment to best practices regarding secure, proper and consistent handling of subscriber's and individual's information; and
- establishing procedures and guidelines to facilitate privacy complaints in instances where a subscriber or individual may be required by the Privacy Commissioner to first contact the Network before lodging a complaint with the Privacy Commissioner.

## 5. General Policy on Publication of Subscriber Details.

5.1 Not withstanding the conditions as defined in Appendix A - Privacy Principals 1 to 10, the Network will make available **ONLY** the following subscriber details:

- **First Name(s) & Last Name(s); and**
- **Callsign; and**
- **Selcall Number**

5.2 To the following persons and/or locations:

- **Base Station Operators for the purpose of operating Base Stations; and**
- **The Printed User List supplied to subscribers and affiliated organisations as part of the Annual Reference Manual; and**
- **Periodic updates as supplied to subscribers and affiliated organisations; and**
- **The User List, as presented on the VKS-737 websites.**

## 6. General Policy Statement on the collection of information.

6.1 Any information collected by the Head Office of the Network either from subscribers or individuals, is stored at the Network's Head Office and is, subject to the conditions as defined in Appendix A – Privacy Principals 1 to 10, and is only available to Head Office staff.

## 7. General Policy Statement on the storage of information.

7.1 All subscription records will be stored on the Network's Head Office Computer Server under the direction of the Administration Manager.

7.2 A daily (held for 7 days) backup copy of the subscription data will be stored in a different building / fire section of the Network's Head Office under the direction of the Administration Manager.

7.3 A weekly backup copy of the subscription data will be stored in a different building / fire section of the Network's Head Office under the direction of the Administration Manager.

7.4 A weekly backup copy of the subscription data will be held securely off-site at a location determined by the Administration Manager.

7.5 A daily (held for 7 days) backup copy of the subscription data will be held securely off-site at a location determined by the Administration Manager.

**Note:** The Network's Administration Manager, Finance Manager, Administration Staff and Honorary Secretary / Public Officer are all required to sign Confidentiality Agreements (From 1st November 2007 all employees will be required to sign confidentiality agreements in accordance with Policy 14 – Employment Conditions Policy).

# Appendix A – Privacy Principles

## 1. Collection

1.1 The Network will not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 The Network will collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) the Network collects personal information about an individual from the individual, the Network will take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, the Network will collect personal information about an individual only from that individual.

1.5 If the Network collects personal information about an individual from someone else, it will take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

## 2. Use and disclosure

2.1 The Network will not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the Network to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the Network to seek the individual's consent before that particular use; and

(ii) the Network will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the Network not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the Network draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the Network with the individual (up to and including the communication that involves the use) sets out the Network's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the Network can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the Network reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the Network has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the Network reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

**Note 1:** It is not intended to deter the Network from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

**Note 2:** Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires the Network to disclose personal information; the Network is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

**Note 3:** The Network is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If the Network uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

- ***child*** of an individual includes an adopted child, a step-child and a foster-child, of the individual.
- ***parent*** of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.
- ***relative*** of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.
- ***sibling*** of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

**3. Data quality**

3.1 The Network will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

## 4. Data security

4.1 The Network will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 The Network will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

## 5. Openness

5.1 The Network will set out in a document clearly expressed policies on its management of personal information. The Network will make the document available to anyone who asks for it.

5.2 On request by a person, the Network will take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

## 6. Access and correction

6.1 If the Network holds personal information about an individual, it will provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the Network may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

**Note:** An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the Network is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If the Network charges for providing access to personal information, those charges:

(a) will not be excessive; and

(b) will not apply to lodging a request for access.

6.5 If the Network holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the Network will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the Network disagree about whether the information is accurate, complete and up-to-date, and the individual asks the Network to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the Network will take reasonable steps to do so.

6.7 The Network will provide reasons for denial of access or a refusal to correct personal information.

## 7. Identifiers

7.1 The Network will not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1a However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances. Note: There are prerequisites that must be satisfied before those matters are prescribed: *see subsection 100(2) of the Privacy Act 1988 (reproduced in Appendix B)*.

7.2 The Network will not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

**Note:** There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: *see subsection 100(2) of the Privacy Act 1988 (reproduced in Appendix B)*.

7.3 In this clause:
***identifier*** includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

## 8. Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

## 9. Transborder data flows

9.1 The Network may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the Network reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the Network, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Network and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the Network has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

## 10. Sensitive information

10.1 The Network will not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or
(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, the Network may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, the Network may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If the Network collects health information about an individual in accordance with subclause 10.3, the Network will take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:
***non-profit organisation*** means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

# Appendix B – Privacy Act 1988 - Section 100

**Regulations**

**(1)** The Governor-General may make regulations, not inconsistent with, prescribing matters:

- **(i)** required or permitted by to be prescribed; or
- **(ii)** necessary or convenient to be prescribed for carrying out or giving effect to this Act.

**(2)** Subject to subsection (3), before the Governor-General makes regulations for the purposes of subclause 7.1A or paragraph 7.2(c) of the National Privacy Principles prescribing an organisation, identifier and circumstances, the Minister must be satisfied that:

- **(a)** the agency or the principal executive of the agency (if the agency has a principal executive) has agreed that adoption, use or disclosure by the organisation of the identifier in the circumstances is appropriate; and
- **(b)** the agency or the principal executive of the agency (if the agency has a principal executive) has consulted the Commissioner about adoption, use or disclosure by the organisation of the identifier in the circumstances; and
- **(c)** adoption, use or disclosure by the organisation of the identifier in the circumstances can only be for the benefit of the individual concerned.

**(3)** Subsection (2) does not apply to the making of regulations for the purposes of paragraph 7.2(c) of the National Privacy Principals if:

- **(a)** the regulations prescribe an organisation, or class of organisations; and
- **(b)** the regulations prescribe an identifier, or class of identifiers, of a kind commonly used in the processing of pay, or deductions from pay, of Commonwealth officers, or a class of Commonwealth Officers; and
- **(c)** the circumstances prescribed by the regulations for the use or disclosure by the organisation, or an organisation in the class, of the identifier, or an identifier in the class, relate to the provision by the organisation of superannuation services for the benefit of Commonwealth officers; and
- **(d)** before the regulations are made, the Minister consults the Commissioner about the proposed regulations.

**(4)** In subsection (3):
"superannuation services "includes the management, processing, allocation and transfer of superannuation contributions.

This Policy Statement has been reviewed and set by the Committee of Management of the Australian National 4WD Radio Network Inc.

**Signed:** 

**Name:** **Steve Johnston OAM**

**Position:** **Administration Manager**

**Date:** **24th August 2007**