

18 June 2009

## **Privacy Policy**

### Australian Meat Industry Superannuation Pty Ltd

ABN 25 002 981 919  
AFS Licence No. 238829  
RSE Licence No. L0000895

as trustee for

### Australian Meat Industry Superannuation Trust

RSE Registration No. R10001778  
ABN 28 342 064 803



**Document control index**

Description	Privacy Policy
Original author(s)	AAS
Creation Date	15 December 2005

**Revision history**

Version	Revision date	Author(s)	Revision notes
2	15 February 2007	Lindy Hunt, Mercer	
3	29 May 2008	Lindy Hunt, Mercer	
4	18 June 2009	Jack Sullivan, AMIST	

**Document sign-off**

Name	CEO signature	Date
Trustee Board	John Livanas	18 June 2009

**Distribution list**

Name	Date
Intranet	18 June 2009

Contents

1.	Your rights to privacy .....	4
2.	What personal information will AMIST keep about me?.....	5
3.	Risks of using the internet.....	6
4.	Collection of browsing information.....	7
5.	Why does AMIST need my personal information? .....	8
6.	Can I see the personal information AMIST has about me? .....	9
7.	How can I contact AMIST? .....	10
	Annexure A.....	11



## **1. Your rights to privacy**

We, the AMIST trustees, understand the importance of protecting your right to privacy and have therefore prepared this statement to help you understand how we aim to protect the privacy of your personal information.

In this document we outline what details we keep about you and why we need these details. Please note that although we refer to “AMIST Super” throughout the document, generally it is Australian Administration Services Pty Ltd (“AAS”) that collects and uses your details on our behalf. AAS is the company that administers AMIST Super (in which you have a superannuation account) on behalf of the AMIST trustees.

In this document we use the term “AMIST Super” which is the “brand name” for the Australian Meat Industry Superannuation Trust. The term “AMIST Super” encompasses AMIST Super (for employer sponsored members), AMIST Super Personal Division and AMIST Pension.

The Privacy Act 1988 (Cth) (“Act”) includes laws that regulate the way organisations, like AMIST and our service providers, handle personal information, including very sensitive information such as health details.

The Act contains 10 National Privacy Principles that regulate, among other things, how organisations collect, store and protect the quality of personal information. Also, how these organisations should use and share personal information with other organisations. The National Privacy Principles form part of all our procedures and policies and the way our members’ accounts are administered.

There is a summary of the National Privacy Principles at Annexure A.



2.

**2. What personal information will AMIST Super keep about me?**

AMIST Super collects personal information from members to administer their accounts. The type of personal information they collect about you includes your name, address, date of birth, telephone number and tax file number.

From time to time additional personal information such as driver's licence and passport may be requested to identify a member under the Anti-Money Laundering and Counter Terrorism Financing Act 2006 and rules.

AMIST Super collects personal information when members use the AMIST Super website to lodge their forms, such as membership application and change of personal details forms, or if members send AMIST Super documents containing personal information. There may also be circumstances when your employer may send personal details to AMIST Super for you.



**3.**

**3. Risks of using the internet**

You should note that there are security risks in transmitting information via the internet. You should assess these potential risks when deciding whether to use our on-line services. If you do not wish to transmit information via the AMIST Super website, there are other ways in which you can provide this information, such as by mail, telephone or on-site visit.

A large grey square containing the number '4.' in white, indicating the start of section 4.

#### **4. Collection of browsing information**

When you browse the AMIST Super website, the following information is logged for statistical purposes:

- your service address;
- top level domain name (for example .com, .gov, .au etc);
- the date and time of your website visit;
- the pages you looked at;
- the documents you downloaded;
- the previous site you visited; and
- the type of browser you used.

We will not try to identify users or their browsing activities except, in the event of an investigation, where a law enforcement agency may exercise a warrant to inspect the service provider's logs.

The AMIST website is “cookie” free, which means we will not send you any unsolicited information after you have accessed our website.

We will only record your email address if you send us a message. It will not be added to a mailing list.

5.**5. Why does AMIST Super need my personal information?**

The personal information AMIST Super collects about you, on our behalf, is used to establish an AMIST Super membership account, to process contributions to your account, to correspond with you and to provide you with superannuation benefits and options from AMIST Super.

If you choose not to provide your personal information, it may mean that we will not be able to provide these services to you, including some AMIST Super benefits and options.

There are other organisations that are connected to the administration services we provide to you and which may have access to your personal information. They are:

- Mailing companies – organisations contracted to do all mailing for AMIST Super.
- Archiving companies – organisations contracted to ensure that all documents are stored in a secure environment.
- Auditors and Regulators – organisations that ensure AMIST Super is complying with legislation and contractual obligations, such as the Australian Taxation Office, the Australian Prudential Regulation Authority, the Australian Transaction and Reports Analysis Centre, the Australian Securities and Investments Commission and the Australian Transaction Reports and Analysis Centre (AUSTRAC).
- Insurance companies – organisations that provide insurance cover for AMIST Super members.



**6.**

**6. Can I see the personal information AMIST Super has about me?**

Under the National Privacy Principles, you have a right to know what information AMIST Super holds about you, and you are entitled to see this information to ensure it is correct. To obtain this information, please contact AMIST Super to ask them for your personal details. The Privacy Act gives limited circumstances in which some or all access to this information may be denied. If this applies to you, AMIST Super will explain this to you when you ask for your information.

A grey square containing the number '7.' in white.

## **7. How can I contact AMIST Super?**

If you want further information on how AMIST handles personal information, or if you want to complain about a possible breach of privacy, please contact AMIST in one of the following ways:

**Write to:**

AMIST Super  
Privacy Officer  
Locked Bag 5390  
PARRAMATTA NSW 2124

**Email:**

amist@as.com.au

**Visit AMIST Super at:**

1A Homebush Bay Drive  
RHODES NSW 2138

**By fax:**

1300 855 378

If you are unsatisfied with the resolution of any complaints, you can refer the matter to the Privacy Commissioner by calling 1300 363 992.

---

## **Annexure A**

### **Information Sheet 2 – National Privacy Principles (NPPs)**

#### **Office of the Federal Privacy Commissioner**

**Summary only: not the full version of the NPPs**

#### **NPP 1 – Collection**

Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, that the person can get access to their personal information and what happens if the person does not give the information.

#### **NPP 2 – Use & Disclosure**

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

#### **NPP 3 – Data Quality**

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to date.

#### **NPP 4 – Data Security**

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.

#### **NPP 5 – Openness**

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

#### **NPP 6 – Access & Correction**

Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.

#### **NPP 7 – Identifiers**

Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government 'agency'.

#### **NPP 8 – Anonymity**

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do.

#### **NPP 9 – Transborder Data Flows**

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

#### **NPP 10 – Sensitive Information**

An organisation must not collect sensitive information unless the individual has consented, it is required by law or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety).

---

## National Privacy Principles

(Extracted from the Privacy Act 1988)

### 1. Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must 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) an organisation collects personal information about an individual from the individual, the organisation must 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, an organisation must collect personal information about an individual only from that individual.
- 1.5 If an organisation collects personal information about an individual from someone else, it must 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 An organisation must 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 organisation 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 organisation to seek the individual's consent before that particular use; and
    - (ii) the organisation 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 organisation not to receive direct marketing communications; and
    - (iv) in each direct marketing communication with the individual, the organisation 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 organisation with the individual (up to and including the communication that involves the use) sets out the organisation'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 organisation 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 organisation 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 organisation 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 organisation 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 organisations 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 an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation 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 an organisation 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

An organisation must 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 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 4.2 An organisation must 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 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.
- 5.2 On request by a person, an organisation must 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 an organisation holds personal information about an individual, it must 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;
  - (k) 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 organisation 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 organisation 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 an organisation charges for providing access to personal information, those charges:
- (a) must not be excessive; and
  - (b) must not apply to lodging a request for access.
- 6.5 If an organisation 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 organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

## 7. Identifiers

- 7.1 An organisation must 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).

- 7.2 An organisation must 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).

- 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

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

An organisation in Australia or an external Territory 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 organisation 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 organisation, 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 organisation 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 organisation 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 An organisation must 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, an organisation 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, an organisation 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 an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must 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.



Australian Meat Industry Superannuation Pty Ltd ABN 25 002 981 919

**Postal Address:** GPO Box 4293, Sydney NSW 2001

**Street Address:** Level 4, 165 Phillip Street, Sydney NSW 2000

**Member Services Hotline:** 1800 808 614

**Phone:** (02) 9230 1100

**Fax:** (02) 9230 1111