NORWOOD INDUSTRIES PTY LTD

PERSONAL INFORMATION MANAGEMENT PROCEDURES

1. Purpose

1.1. Norwood Industries Pty Ltd ("Norwood") respects and upholds the rights to privacy protection under the National Privacy Principles contained in the *Privacy Act 1988*. The National Privacy Principles apply to Norwood from their introduction on 21 December 2001.

1.2. The National Privacy Principles outline the way in which personal information is to be collected, used, stored and destroyed. A summary of the National Privacy Principles is attached at the end of this Policy document for you to read.

1.3. This Policy describes how Norwood will manage personal information they collect from people who are **not** employed by Norwood.

1.4. This Policy may be amended from time to time as the management sees fit.

2. Scope

2.1. This Policy describes how Norwood deals with personal information and as such applies to all employees, officers and agents of Norwood.

2.2. This Policy should also apply to any contractor collecting or dealing with information on behalf of Norwood.

3. Privacy Coordinator

3.1. Norwood has appointed a Privacy Coordinator to assist staff in complying with this Policy. If at any time you have any questions relating to any aspect of this Policy or you are unsure how to deal with a piece of personal information, the Privacy Coordinator is available during office hours to assist you. Norwood Australia's Privacy Coordinator is the Human Resources Officer

4. Key Concepts

4.1. "**Personal information**" is information about an individual from which the individual's identity is apparent. This can be in any form, such as photos, computer graphics, letters, file notes and videos. Examples of personal information include a tape recording where a person's name is mentioned or an email from a customer from which their identity can be ascertained.

4.2. "**Health information**" is information or an opinion about the health or disability of an individual, an individual's expressed wishes about the future provision of health services to him or her or a health service that is, or will be, provided that is also personal information.

4.3. "**Sensitive information**" is personal information which includes information about an individual's racial or ethnic origin, political or religious beliefs, membership of a professional or trade association or union, sexual practices, criminal record or health information. As a general guide, sensitive information can be considered "politically correct" information and jokes or remarks that touch upon such information may offend some people.

5. Collection

5.1. Collection of Personal Information Generally

(1) Personal information should only be collected to the extent that Norwood has a legitimate purpose for collecting the information relating to the functions or activities of Norwood.

(2) Norwood does not collect personal information covertly or in an unreasonably intrusive manner. All collectors of personal information should use every effort to ensure that no intimidation or deception is made in connection with collecting personal information.

(3) Where it is reasonable and practicable to do so, personal information about an individual should only be collected directly from the individual. In deciding whether or not it is reasonable and practicable to collect personal information directly from the person you should consider the following:

(a) whether it is possible to collect the information directly from the person;

(b) whether a reasonable person might expect the information to be collected from them directly or indirectly;

(c) how sensitive the information is;

(d) the cost to Norwood of collecting the information directly rather than indirectly;

(e) the privacy consequences for the individual if the information is collected indirectly rather than directly; and

(f) what is accepted industry practice.

If you are not sure whether is it is reasonable or practicable to collect personal information directly from the individual, contact the Privacy Coordinator.

(4) Where personal information is collected from a third party outside Norwood, reasonable steps should be taken to ensure that the individual is, or has been made, aware of the issues in item 5.2 or 5.3 (as the case may be).

(5) Sensitive information should not be collected from an individual without their consent. If it is necessary to collect information to meet an individual's specific needs (eg. taste preferences), such information could be collected in a way that does not necessarily involve collecting "sensitive information". For instance, the individual might be asked about the language they speak or dietary preferences rather than asking about the individual's ethnic origin or religious beliefs.

(6) Norwood does not believe it is necessary to collect sensitive information for the operation of Norwood and its related organisations. If you believe that sensitive information needs to be collected for a particular purpose, the Privacy Coordinator must be consulted beforehand, and his or her decision complied with.

(7) Reasonable steps should be taken to ensure that the personal information is accurate, complete and up-to-date when the information is collected, used or disclosed. Personal information need not be checked at other times (unless it is requested under part 0). Factors that should be considered when deciding whether personal information is accurate, complete and up-to-date include:

(a) how likely it is that the personal information is accurate, complete and up-to-date;

(b) whether this kind of personal information changes over time;

(c) how recently the personal information was collected;

(d) how reliable the personal information is likely to be;

(e) who provided the personal information (eg. was it the person him/ herself?); and

(f) what the personal information is going to be used for.

If personal information is used soon after collection, that information may not need to be checked. Where personal information is provided from another person (eg. a relative or friend of the person), there may be a greater need to check that the personal information is accurate, complete and up-to-date.

(8) Government allocated identifiers (eg. Medicare number) are not to be used to identify an individual and are not to be used as Norwood' identifiers. Government allocated identifiers should not be disclosed to third parties unless required by law.

(9) Where possible and where appropriate, the individual should be given the choice of "opting-in" or "opting out" of future activities or use of their information when personal information is collected. For instance, a statement to the effect "tick this box if you do not wish to receive further information on this product" or (verbally) "would you like to receive more information on XXX?" would be sufficient. The "opt-out" choice should be clearly and prominently presented and unambiguous.

(10) Norwood does not impose any extra charge on an individual for "opting-out" under item 5.1(9). An "opt-out" choice should be freely available and not bundled together with other purposes.

5.2. Collecting Personal Information Orally

When personal information is collected, the individual needs to be made aware of certain matters. This can be accomplished by following the following procedures:

(1) The individual should be told who is collecting their personal information at the time such personal information is being collected. For instance, "My name is XXX and I am calling from Norwood" or "Norwood, XXX speaking". Where personal

information is being collected on behalf of another organisation, the individual must be advised.

(2) The individual should be told that he or she is able to gain access to the personal information they provide.

(3) The individual should be told the reason or reasons for collecting their personal information. The reasons can be quite general, so long as the individual is aware of what Norwood is going to do with the information (eg. entering the individual into a competition).

(4) The individual should be told about the organisations to which such personal information is usually disclosed.

(5) Where applicable, the individual should be told about any law that requires the individual to provide, or Norwood to collect, personal information in a particular situation. The specific piece of legislation need not be referred to (although this is preferable). For instance, a statement such as “XXX law requires that we collect this” is acceptable.

(6) The individual should be told the main consequences if he or she does not provide all or part of their personal information. Not all possible consequences need to be described. Often this means making it clear what items are essential to fulfil the purposes of the collection. For instance, a statement to the effect, “if you don’t tell us this, we will be unable to enter you into our competition” is sufficient.

(7) If it is possible for the individual to transact anonymously with Norwood, the individual should be made aware of that.

5.3. Collecting written and electronic information.

When personal information is being collected, the individual needs to be made aware of certain matters. This should be done at the time of collecting the personal information, or as soon as possible after it has been collected. This can be accomplished by following the following procedures:

(1) The form or website should make it clear to the individual that Norwood is collecting his or her personal information. Where personal information is being collected on behalf of another organisation, the form or website should make that clear.

(2) The form or website should inform the individual that he or she is able to gain access to the personal information they provide.

(3) The form or website should state the reason or reasons for collecting the personal information. The reasons can be quite general, so long as the individual is aware of what Norwood is going to do with the information. For instance, a reason may include entering the individual into a competition.

(4) The form or website should make it clear to the individual which organisations the personal information is being disclosed to.

(5) Where applicable, the form or website should inform the individual about any law that requires the individual to provide, or Norwood to collect, personal information in a particular situation. The specific legislation need not be referred to (although this is preferable). For instance, a statement such as “XXX law requires that we collect this” is acceptable.

(6) The form or website should outline the consequences for the individual if he or she does not provide all or part of their personal information. Not all possible consequences need to be described. Often this means making it clear what items are essential to fulfil the purposes of the collection. For instance, a statement to the effect “if you don’t tell us this, we will be unable to enter you into our competition” is sufficient.

(7) If it is possible for the individual to transact anonymously with Norwood, the form or website should specify that.

6. Storage of Personal Information

6.1. All personal information collected by Norwood needs to be protected from misuse, and loss, and unauthorised access, modification and disclosure.

6.2. Paper based personal information should be stored in the following way:

(1) Customer account application forms are filed in lever arch files.

(2) Credit card payment information and debt collection agency information is retained in a lockable filing cabinet.

(3) Sales consultants receive account information about customers. This information is kept in the customer folder and is not shown to a third party. The original account application forms have to be mailed to the head office.

6.3. Electronic information should be stored in the following way:

(1) Electronic information in stored in specific program packages the packages are password protected. Only authorised people have access.

(2) The data is backed up from time to time. The data is stored at a specialised security company.

7. Security Procedures relating to Personal Information

7.1. The following security procedures are to be followed in relation to the storage of paper based personal information:

(1) All sensitive paper based information is stored in lockable cabinets. Only authorised people have access.

7.2. The following security procedures are to be followed in relation to the storage of electronic personal information:

(1) Electronic personal information is stored in specific programs which are password protected.

8. Use and Disclosure of Personal Information

8.1. Primary and Related Purposes

(1) Personal information collected from an individual should, generally, only be used for the primary purpose or purposes for which it was collected. A primary purpose is basically the reason for the transaction. For instance, a primary purpose might be the entering of the individual into a competition, or assessing the individual for prospective employment.

(2) Personal information can be used for a secondary or related purpose to the primary purpose. A secondary or related purpose is something that arises in the context of the primary purpose or doing what is necessary to complete the transaction in a way that an individual would reasonably expect. When thinking about whether the use of the personal information is for a primary or secondary purpose, the following should be considered:

(a) the context in which the personal information is collected;

(b) the reasons given to the individual about why his or her personal information is being collected; and

(c) how sensitive or confidential the information is.

A good test is to put yourself in the shoes of the individual and ask yourself, “if I were not working here and had no knowledge of this industry, in the circumstances, how would I expect my information to be used?”.

(3) Where **sensitive information** is involved, the Privacy Coordinator should be consulted before using or disclosing such information.

(4) Information about a person in their business role that is used and disclosed for generally accepted business purposes is considered within an individual’s reasonable expectations. For example, an exchange of business cards and use of them subsequently for business contacts is permissible.

8.2. Secondary Use and Disclosure With Consent

(1) Personal information can be used for a secondary or related purpose (see 8.1(2) for meaning of “secondary or related purpose”) if the individual has consented.

(2) Consent under 8.2(1) can be either express or implied. Express consent is where the individual notifies Norwood straightforwardly, verbally, in writing or via the internet, that he or she consents to the proposed use of their personal information. Implied consent is where consent may be reasonably inferred from the conduct of the individual. For instance, it is possible to infer consent from the individual’s failure to “opt-out” (where the opt-out complies with items 5.1(9) and 5.1(10) of this policy).

(3) Where the use or disclosure of the personal information for a secondary or related purpose might have serious consequences for the individual, the express consent of the individual should be obtained.

(4) When deciding whether or not to infer an individual's consent, the following should be considered:

(a) the likelihood of the individual having received and read the information, or having been verbally informed, about the use or disclosure of the personal information;

(b) the chance to "opt-out" and the likelihood of the individual understanding the consequences of not "opting-out"; and

(c) whether the consequences of failing to "opt-out" are harmless.

8.3. Direct Marketing

(1) Personal information, **not** sensitive information, can be used for direct marketing in the following circumstances:

(a) Where it is impracticable to obtain the individual's prior consent. The question of impracticability should be considered at the time of the proposed use of the personal information rather than when it was collected, and the following factors should be considered:

(i) how often, and in what way, does Norwood communicate with the individual;

(ii) the consequences for the individual of receiving the information without having consented; and

(iii) the cost to Norwood of seeking consent.

It is **not** considered impracticable to seek consent via email.

(b) Where the individual has not opted out previously of receiving marketing information from Norwood.

8.4. Use or Disclosure by Law

(1) Where Norwood is required by law to use or disclose personal information (for instance in a criminal investigation), such information must be disclosed.

(2) Where Norwood is authorised by law to use or disclose personal information, such information may be disclosed after consultation between the Privacy Coordinator, management and Norwood' legal advisers.

8.5. Primary purpose and Related Companies

(1) Personal information can be disclosed to companies related to Norwood, that is, without such disclosure being a breach of privacy.

(2) The primary purpose of the original collection of the personal information remains with the personal information even after it is disclosed to a related company. That is, the related company that receives the personal information must treat that information as if it were the company that originally collected that information.

(3) Where a related company wishes to use or disclose the personal information it receives under item 8.5(1), that company must comply with part 8 of this policy, as if it were the company that originally collected the information.

8.6. Other Reasons For Disclosure

(1) The National Privacy Principles provide examples of other instances of where personal information may be disclosed, for instance, in situations where there is a serious threat to health and safety and disclosure of such information will help reduce that threat. Norwood considers reasons other than items 8.1 to 8.5 for disclosing personal information to be negligible.

(2) Where you consider that there are reasons for disclosing personal information other than for matters outlined in items 8.1 to 8.5, the Privacy Coordinator should be consulted.

8.7. This privacy policy applies to all personal information.

9. Sending Personal Information Overseas

9.1. The National Privacy Principles only allow personal information to be sent overseas if that overseas country has laws, or an arrangement is in place, which offers similar protection to personal information as in Australia.

9.2. If you want to transfer personal information to other Norwood organisations outside of Australia, the following provisions must be complied with:

(1) At this current date we do not send any information overseas. If circumstances change a policy will be implemented.

9.3. If it is necessary to send personal information overseas to a person or a company that is not related to Norwood, check with the Privacy Coordinator that it is permissible to send the personal information to the intended recipient(s).

10. Individuals Wanting to Know About Norwood' Policy

10.1. Norwood has a standard policy in place, which explains generally how Norwood deals with personal information. This policy should be sent to an individual if he or she requests it. This external policy can be found in all staff guidelines as well as on the website – www.Norwood.com.au.

10.2. Where an individual inquires about the information that Norwood holds about him or her, he or she should be told generally the information that Norwood has, and what that

information is used for. For instance, an individual might be informed that Norwood has an individual's contact details and age for use in competitions.

11. Requests for Access to Personal Information

11.1. **Only** the Privacy Coordinator or other person appointed by Norwood may consider a request for access to personal information.

11.2. All requests for access to personal information are to be passed on to the Privacy Coordinator as soon as possible after a request has been made.

12. Providing Access to Personal Information

12.1. Individuals generally have the right to access their personal information that Norwood holds about them on request, although there are instances when Norwood does not have to grant the individual access to their personal information.

12.2. Norwood does not charge an individual for lodging a request to access their personal information. Norwood does not ordinarily charge an individual for providing access to their personal information, but may do so depending on the circumstances.

12.3. Where Norwood receives a request in writing or via email by an individual requesting access to their information, the Privacy Coordinator must acknowledge their request within 14 days of receiving such a request, to the effect that Norwood has received the individual's request for access to their personal information and that the request is being considered by the Privacy Coordinator.

12.4. If an individual requests access to their information, the Privacy Coordinator should first check whether the exceptions in item 12.5 apply. If an exception does apply, the individual should be notified in accordance with item 12.10. Where access is to be granted to the individual, this should be done as soon as possible, but at any rate no longer than 30 days after receiving the request for access.

12.5. The following are circumstances in which Norwood does not have to give an individual access to their personal information:

(1) Where providing personal information would unreasonably impact on the privacy of another individual. This could be any information from which the identity of another person could be identified.

(2) Where a request is frivolous or vexatious (eg. trivial or for amusement's sake, or a repeated request for the same information). However, a request is **not** frivolous or vexatious merely because it is irritating.

(3) Where legal dispute resolution proceedings are underway or are anticipated and the process of discovery would not permit access to the personal information.

(4) Where Norwood is negotiating with the individual and providing access to personal information would prejudice or interfere in some negative way Norwood's negotiations or show the intentions behind such negotiations.

(5) Where providing personal information would be unlawful.

Where denying access to personal information is required or authorised by law.

(6) Where unlawful activity (eg. fraud, theft) is reasonably suspected and providing personal information is likely to prejudice an investigation into that unlawful activity.

(7) Where a law enforcement body directs Norwood not to provide an individual with access to their personal information.

(8) Where providing access to personal information would reveal a commercially sensitive decision making process of Norwood, Norwood can give the individual an explanation for the commercially sensitive decision rather than direct access to the information. However, this does **not** permit Norwood from denying the individual factual personal information on which commercially sensitive decisions have been based. This item 0 can **only** be relied when there is a genuine commercially sensitive decision making process involved.

(9) The National Privacy Principles provide other instances where access to personal information may be denied, such as, if there is a serious threat to the life or health of any person, but Norwood considers such instances to be highly unlikely.

12.6. Where Norwood is not required to provide an individual with access to their personal information under parts 12.5(1) to 12.10, an intermediary that is acceptable to both Norwood and the individual should be considered. For instance, this may involve having the individual's lawyer or accountant accessing the information. Where an intermediary is considered, consideration should be given to having a confidentiality agreement in place in appropriate circumstances. Where an intermediary is being considered, it may be appropriate to consult with Norwood' legal advisers.

12.7. Norwood may charge the individual for providing access to their personal information. Such a charge (if any) must be reasonable and must **not** apply to the individual's lodging of a request for access.

12.8. Where an individual establishes that his or her information held by Norwood is not accurate, complete and up-to-date, reasonable steps must be taken to ensure that the personal information is accurate, complete and up-to-date.

12.9. Where there is a disagreement between Norwood and an individual over whether personal information is accurate, complete and up-to-date, and the individual requests that a statement be associated with the information claiming that the information is not accurate, complete and up-to-date, reasonable steps must be taken to do so (eg. placing such a statement in the individual's file).

12.10. The individual must be given the reasons for denying him or her access to their personal information or refusing to correct his or her personal information. In explaining the reasons for denying such access, the individual should be informed as to which exception has been relied upon under item 12.5.

Reasonable steps should be taken to ensure that the individual seeking access to personal information is in fact the individual the personal information is about. Only the individual is to have access unless a valid and acceptable reason is given to Norwood. Where the individual personally attends Norwood to access personal information, a form of photo identification (eg. driver's licence) will need to be checked.

13. Destruction or De-Identification of Personal Information

13.1. Personal information that is no longer required for any relevant purposes as outlined under item 8 should be destroyed or de-identified. However, simply because a particular transaction has been completed, this does not necessarily mean that a relevant purpose no longer exists. It is appropriate in many circumstances to keep personal information for future reference. The following are some examples where a relevant purpose exists and the information does not need to be destroyed or de-identified:

(1) Where an individual has applied for unsuccessfully for a job at Norwood, it may be appropriate to keep his or her personal information for future reference, for instance, to notify him or her about an appropriate position that is vacant.

(2) Data collected from research undertaken may need to kept for future reference, even though the research exercise is complete. This may be necessary, for example, to compare it with future research.

In deciding whether a relevant purpose exists, the original reasons for collecting that information should be considered as well as the reasons why such information might need to be kept. If you are not sure whether it is appropriate to keep certain personal information, contact the Privacy Coordinator.

13.2. Paper based personal information has to be shredded. Where impractical to shred the documents must be placed in the security destruction bins.

Paper based information keep by the salesforce is to be destroyed by tearing into small pieces and placed into the rubbish bin. Upon disposal you must be satisfied that the information could not be recognised by a third party.

13.3. Electronic personal information should be erased in the following way:

(1) The personal information should be deleted from the server and all back up copies erased. This includes emails, file notes, computer graphics and cookies.

(2) Any disks or cd-roms containing personal information must be erased.

13.4. De-identification is the removal of any information from which an individual may be identified from a record.

13.5. De-identification must be permanent so that it is not possible to match the de-identified information with other records to establish the identity of the person. This may be as simple as destroying or erasing that part of the information from which a person can be identified (name, age, address etc).