

Solo Group takes its obligations under the Privacy Act seriously and seeks to take all reasonable steps in order to comply with the Act and protect the privacy of the personal information that we hold. This policy sets out how we intend to achieve this.

Solo Group collects and holds personal information about:

- Customers
- Suppliers
- Employees

## **PRIVACY STATEMENT**

Solo Group and its associated companies and trusts are covered by 10 National Privacy Principles, the NPP's, as set out in the Privacy Act 1988 (amended by the Privacy Amendment (Private Sector) Act 2000). The NPP's set out how private sector organisations should collect, use, keep secure and disclose personal information. The principles give individuals a right to know what information an organisation holds about them, and a right to correct that information if it is wrong. Below is a summary of the NPP's that relate to Solo Group. For more detail please go to: <http://www.privacy.gov.au/materials/types/infosheets/view/6583>.

### **Collection**

Any personal information collected is collected by Solo Group. This may include video or photographic images. Security cameras located in workshops or processing plants may collect images on a random basis for security reasons.

### **Use and Disclosure**

Other personal information may be collected for the purposes of selling our products or services, processing payment, collecting debts or to perform obligations under a contract with another party (e.g. in the course of providing services under a domestic garbage contract for a local authority) and performing payroll or personnel functions for a related company or trust or as a sub-contractor.

Solo Group may disclose relevant information to our insurers, as required by legislation and to our contractors to perform their functions.

Individuals are not obliged to give us personal information. However, if individuals do not provide Solo Group with the relevant personal information, we may not be able to provide the service or complete the transaction.

### **Data Quality and Security**

Solo Group is committed to ensuring that personal information collected remains accurate, complete, up to date and secure. We will take all reasonable steps to protect the security of the information that we hold. This includes appropriate measures to protect electronic material and materials stored and generated in hard copy. Records that are no longer required are destroyed.

We may contract out data storage or processing functions. If Solo Group does contract out, we will take measures to protect the information by ensuring that the contracting organisation has an appropriate Privacy Policy, and has signed a Privacy Statement.

When dealing with sensitive information (health, racial, ethnic background or criminal record), higher standards of security will apply.

### Openness

Solo Group will upon request, inform a person generally about what information it holds concerning that person and for what purpose such information is held.

### Access and Correction

Solo Group provides employees with a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date. Access to personal information will only be granted to those requesting information about themselves. To obtain access individuals must provide proof of identity.

### When will Access be denied?

Access will be denied if:

- the request does not relate to the personal information of the person making the request;
- providing access would pose a serious and imminent threat to life or health of a person;
- providing access would create an unreasonable impact on the privacy of others;
- the request is frivolous and vexatious;
- the request relates to existing or anticipated legal proceedings
- providing access would prejudice negotiations with the individual making the request;
- access would be unlawful;
- denial of access is authorised or required by law;
- access would prejudice law enforcement activities;
- access discloses a 'commercially sensitive' decision making process or information; or
- any other reason that is provided for in the National Privacy Principles (NPPs) set out under the Privacy Act.

Where possible, Solo Group will favour providing access. It may do so by providing access to the appropriate parts of the record or by using an appropriate 'intermediary'.

Where there is a dispute about the right or forms of access these will be dealt with in accordance with the Solo Group *Grievance Reporting Procedure (IMS-HRPR-D-6002)*.

### Time

We will take all reasonable steps to provide access within 30 days of your request.

## Costs and Charges

Solo Group may impose the following charges:

- Photocopying – \$0.50 per page
- Delivery cost of information stored off-site – where information is stored off-site, the cost of obtaining access to the information - \$20
- Access to electronic databases – \$10

## Transborder Data Flows

Solo Group does not send any personal information overseas.

## PRIVACY COMPLAINTS

Solo Group realises the importance of privacy to the organisation, its customers and other stakeholders. As such we are committed to protecting the privacy of the personal information that we hold. This is part of our organisations:

- (a) Legal obligation under the Privacy Act 1988.
- (b) Ethical and business obligations.
- (c) Service to our customers, suppliers and employees.

Solo Group places high priority on effectively handling any complaints dealing with privacy that individuals may have.

If an individual has any complaints about our privacy practices, or wishes to make a complaint about how an individual's personal information is managed, he / she should contact the Administration Manager at Head Office.

## Overriding Principles

At all times the conduct under this policy will be governed by the following principles:

- (a) All complaints will be treated seriously, promptly and in a confidential manner.
- (b) The privacy complaint will not have an effect on the individuals existing obligations or the commercial arrangements that exist between this organisation and the individual.

## Who May Complain Under This Policy?

If an individual has provided us with personal information he/she has a right to make a complaint and have it investigated and dealt with under this policy.

## What is a Privacy Complaint?

A privacy complaint relates to any concern or dispute that an individual has with our privacy practices as it relates to his/her personal information. This could include matters such as:

- (a) How personal information is collected.
- (b) How personal information is stored.
- (c) How this information is used or disclosed.

(d) How access is provided.

### Treatment of Complaints about Privacy Practices

Solo Group seeks to resolve grievances as quickly as possible. If individuals have a complaint about privacy they should contact the Administration Manager.

All complaints will be logged in a complaints register.

Complaints must be in writing, addressed to the Administration Manager. All unresolved complaints come to the attention of The Managing Director.

### Grievance Procedure for Privacy Complaints

The goal of this policy is to achieve an effective resolution of complaints within a reasonable set timeframe (30 days or as soon as practicable).

Once a complaint has been made, the point of contact can then resolve the matter in a number of ways:

1. Request further information: We may request further information. Individuals should be prepared to give as many details as possible including details of any relevant dates and documentation. This will enable us to investigate the complaint and determine an appropriate and useful solution. All details provided will be kept confidential.
2. Discuss options: We will discuss options for resolution and if the individual has suggestions about how the matter might be resolved this should be discussed with the Privacy Officer or your immediate supervisor. We could also suggest other solutions or give examples of how the personal information can be revised or stored in a different way.
3. Investigation: The complaint may be investigated. The organisation will do so as soon as possible. It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to deal with the complaint.
4. Escalate internally: If a complaint can't be resolved it will be referred to the Managing Director. This will be discussed with the individual before the referral.
5. Discussion with any other parties: If the complaint deals with the conduct of our employees we will raise the matter with the employee concerned and seek their comment and input in the resolution of the complaint.
6. The complaint is resolved: If the complaint is found to be substantiated, the individual will be so informed. Solo Group will then take appropriate steps to resolve the complaint and prevent the problem from recurring.
7. If the complaint is not substantiated, or cannot be resolved to the individual's satisfaction, but this policy has been followed, the decision of
8. Resource Recovery will be final. The Privacy Officer will discuss the reasons for the decision with the individual.
9. If there is still disagreement the complaint will be dealt with by a mutually agreed independent intermediary.
9. If after all the above steps have been followed the complaint is unresolved the individual is free to take your complaint formally to the Federal Office of the Privacy Commissioner.

## **Records**

The organisation will keep a record of individual's complaints and the outcomes.

## **Anonymous Complaints**

Solo Group is unable to deal with anonymous complaints as we are unable to investigate properly and follow-up such complaints.