PRIVACY POLICY

DOCUMENT CONTROL TABLE

Document Owner:	Corporate Services	**Section:**	Corporate Services
Endorsed by:	Executive Leadership Team	**Date:**	16 March 2021
Approved By:	Metro Board	**Date:**	31 March 2021
Next Review Due:	31 July 2022		

Contents

1 PURPOSE

Metro Tasmania (Metro) is committed to complying with its obligations under the *Privacy Act* 1988 (*CTH)* (Privacy Act), including the Australian Privacy Principles (APPs) and the *Personal Information Protection* Act *2004 (TAS*) (PIP Act).

This Policy defines the protections in place to protect the personal information we hold about employees, contractors and customers.

Our employees are trained to protect your personal information in accordance with our policies, procedures and systems.

2 SCOPE

This Policy applies to all Metro employees, contractors and our customers.

3 POLICY STATEMENT

We are committed to protecting and maintaining the privacy, accuracy and security of all personal information held.

This undertaking relates to all personal information obtained from customers, employees and others; whether obtained directly from those concerned or via a third party.

This policy explains how we manage and secure personal information. It also describes the types of personal information we hold and for what purposes, and how that information is collected, used and disclosed.

Please read this policy carefully before you provide us with any personal information.

3.1 TYPE OF INFORMATION COLLECTED

Personal Information

In respect of customers, we may collect and hold the following types of personal information:

a) When you visit and log onto our Greencard website we will record the transactions;

b) Identification information including a customer's name, date of birth, postal address, fax number, telephone number, email address and pensioner and concession status;

c) Any complaint details;

d) CCTV footage;

e) Any other information that we consider to be reasonably necessary.

In respect of employees, we may collect and hold the following types of information:

a) Identification information including employee's name, date of birth, postal address, fax number and telephone number, tax file number, bank account, drivers licence details and superannuation fund details;

b) Employment information;

c) Income details;

d) Any complaint details;

e) Any other information that we consider to be reasonably necessary.

Sensitive Information

We may need to collect sensitive information about you. Unless the information is required or authorised to be collected by law, we will only collect sensitive information with your consent.

In respect of customers, we may collect the following types of sensitive information:

a) Bank account details;

b) Date of birth;

c) Centrelink concession detail.

In respect of employees, we may collect the following types of sensitive information:

a) Health information;

b) Criminal records;

c) Bank account details;

d) Personal address.

Information Required by Law

We may collect information about you because the collection of the information is required or authorised by law or a court/tribunal order.

3.2 COLLECTING INFORMATION

We will only collect information by lawful and fair means and not in an unreasonably intrusive way. We collect, hold, use and disclose your personal information for the following purposes:

a) To enable us to provide services to you;

b) To respond to complaints;

c) To manage and deal with any possible legal actions, including dispute resolution purposes;

d) To protect the health and safety of our customers and employees;

e) To manage accounts;

f) To manage human resources;

g) To identify you;

h) To comply with any applicable laws, regulations or code of practice;

i) For any other purpose for which you have given your consent.

We will, if it is reasonable and practicable to do so, collect personal information directly from you. This may happen when:

a) You give us information over the telephone;

b) You interact with us electronically or in person;

c) You access our website;

d) We provide services to you;

e) You complete a Greencard application form;

If you do not provide us with your personal information, we may not be able to:

a) Provide you with the services you want;

b) Verify your identity.

Collecting Personal Information from Other Sources

Sometimes we collect personal information about you from other sources where it is necessary to do so. This may happen where:

a) You have consented to the collection of the information from someone else;

b) We are required or authorised by law to collect the information from someone else; or

c) It is unreasonable or impracticable to collect the information from you personally.

Examples of other sources we may collect personal information from include but are not limited to:

a) For employees: from family members, medical advisors, current and former employers, Medicare, Centrelink, Australian Tax office, government departments and agencies, insurance companies, their authorised representatives, and banks and financial institutions.

b) For customers: from banks and financial institutions, insurance companies or authorised, professional advisors. For customers and employees we may access publicly available information such as from the electoral role, telephone directories or websites.

Unsolicited Personal Information

If we receive personal information about you that we did not ask for, we will check whether that information is reasonably necessary for our functions or activities. If it is, we will handle this information the same way we do with other information we collect from you. If not, we will destroy it or de-identify the information provided it is lawful and reasonable to do so and the information is not contained in a Commonwealth record.

3.3 USING THE INFORMATION

We will not use or disclose your personal information that was collected for a particular purpose for another purpose, unless:

a) You have consented to the use or disclosure of the information for another purpose;

b) You would reasonably expect us to use or disclose the personal information for another purpose;

c) The use or disclosure is otherwise permitted under the *Privacy Act* or the *PIP Act*;

d) The passing of database information to software vendors responsible for the maintenance of the software.

We will not sell or trade your personal information.

We may disclose your personal information to third parties, including, but not limited to, schools, parents or guardians, provided that the reason for the disclosure is directly related to protecting the health and safety of our employees or our customers.

We are not likely to disclose your personal information to any overseas recipients.

Where your personal information is disclosed, we will seek to ensure that information is used, held and disclosed consistently with the Privacy Act and any other applicable laws.

3.4 QUALITY OF INFORMATION

We will take all reasonable steps to ensure that any personal information we collect, hold, and use or disclose is accurate, complete, up to date and relevant to our functions or activities.

If you believe that your personal information is not accurate, complete, up to date or relevant, please contact our Privacy Officer (General Manager Corporate Services) in accordance with Section 3.9 of this Policy.

3.5 SECURITY OF INFORMATION

We store your personal information in different ways, including paper and electronic form.

We treat all personal information as confidential. We will take reasonable steps to ensure that personal information is protected from:

a) Misuse, interference and loss;

b) Unauthorised access, modification and disclosure.

Some of the ways we do this are:

a) Limiting access to personal information to those people who need to know that information;

b) Taking steps to minimise the opportunity for third parties (including unauthorised members of the organisation) to overhear or otherwise become aware of that information;

c) Electronic security systems, such as firewalls and data encryption, user identifiers, passwords, antivirus, antispyware, backup and recovery of systems;

d) Control of access to metro buildings.

If we no longer need your personal information for any purpose, we will take reasonable steps to destroy or permanently de-identify the information, unless:

a) The information is contained in a Commonwealth record;

b) We are required by law, or a court/tribunal order, to retain the information.

As a general guide the law requires us to keep information relating to many aspects of our business for seven years. However, we may retain information for shorter or longer periods depending upon specific legal requirements or the needs of our business.

3.6 ACCESS TO INFORMATION

You can access your personal information, unless an exception in the *Privacy Act* or the *PIP Act* applies (e.g. where giving access would have an unreasonable impact on the privacy of others, the request is frivolous or vexatious or the information relates to existing or anticipated legal proceedings and might otherwise prejudice those proceedings, or negotiations between the parties).

You can request access to your personal information by contacting our Privacy Officer (General Manager Corporate Services) in accordance with Section 3.9 of this Policy.

Depending upon the nature of the request we may charge you a small fee to cover our costs when giving you access. We will endeavour to advise you of the cost (if any) before we process your request.

We will respond to a request for access within a reasonable time (usually within 30 days), and give access in the manner requested by you, if it is reasonable and practicable to do so.

3.7 CORRECTION OF INFORMATION

Sometimes human errors can occur in the data we hold, or in our application of this policy. If you think that any personal information we hold about you is incorrect, inaccurate, incomplete and out-of-date, irrelevant or misleading, you may request us to correct the information by contacting the Privacy Officer (General Manager Corporate Services) in accordance with Section 3.9 of this Policy.

We will take reasonable steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

If we correct personal information that has been disclosed to another entity and you ask us to tell the other entity about the correction, we will take reasonable steps to tell the other entity about the correction, unless it is impractical or unlawful to do so.

If we refuse to correct the personal information, then we will provide you with:

a) Written reasons for the refusal provided it is reasonable to do so;

b) The mechanisms available to complain about the refusal

We must respond to a correction request within a reasonable time (usually within 30 days).

3.8 ANONYMITY

You have the option to remain anonymous, or to use a pseudonym, when dealing with us where it is lawful and practical to do so

3.9 PRIVACY ISSUES

If you:

a) Have any issues about the way we handle your personal information after reading this policy;

b) Become aware of a potential breach of privacy;

c) Wish to make a complaint please contact our Privacy Officer (General Manager Corporate Services) as set out below:

Privacy Officer
Telephone: (03) 6233 4205
Email: privacy.policy@metrotas.com.au
Mail: Metro Tasmania, PO Box 61, Moonah, TAS, 7009

We aim to respond to any privacy issues within 10 business days.

If the Privacy Officer (General Manager Corporate Services) is unable to resolve the matter, it will be escalated (internally or externally) as appropriate to facilitate resolution.

3.10 REPORTING ELIGIBLE DATA BREACHES

An eligible data breach is either:

a) Unauthorised access or disclosure of your information or information that relates to you that a reasonable person would conclude is likely to result in serious harm to you; or

b) Where your information or information that relates to you is lost in circumstances where unauthorised access or disclosure of information is likely to occur and it can be reasonably concluded that such an outcome would result in serious harm to you.

If we suspect that there has been an eligible data breach we will carry out a reasonable and expeditious assessment.

If we have reasonable grounds to believe that there has been an eligible data breach we will notify you and the Office of the Australian Information Commissioner and will provide:

a) A description of what occurred;

b) The kinds of information concerned; and

c) Recommended steps that you should take in response to the data breach.

3.11 EXTERNAL COMPLAINT MECHANISM

If you are not happy with the outcome of the Privacy Officer's (General Manager Corporate Services) investigation or we have not replied to you within a reasonable, then you can raise your concern with the Office of the Australian Information Commissioner (OAIC)

Complaints can be made to OAIC in the following ways:

Office of the Australian Information Commissioner
Telephone: 1300 363 992
Email: enquiries@oaic.com.au
Mail: GPO Box 5218 Sydney NSW 2001
Online: https://www.oaic.gov.au/privacy/privacy-complaints/

4 RESPONSIBILITIES

4.1 COMPLIANCE, MONITORING AND REVIEW

It is the responsibility of:

- The General Manager Corporate Services, as the Privacy Officer, to review this Policy;
- The Executive Leadership Team to endorse this Policy; and
- The Metro Board to approve this Policy.

4.2 REPORTING

Any breaches of this Policy will be reported to the Chief Executive Officer.

4.3 RECORDS MANAGEMENT

Metro must maintain all records relevant to administering this policy in Metro's Electronic Records and Document Management System, *Content Manager.*

5 REVIEW PERIOD

This Policy will be reviewed annually or earlier if required.

6 RELATED AND REFERENCED DOCUMENTS

6.1 LEGISLATION

Personal Information Protection Act (TAS) 2004

Privacy Act 1988 (CTH)

Privacy Regulations 2013 (CTH)

6.2 METRO

Code of Conduct Procedure

7 VERSION CONTROL TABLE

No:	Date	Details	Status
1	23/08/19	Reviewed by Edge Legal and advised to add examples of other sources Metro may collect personal information from. Endorsed by EMT and approved by the Board.	Superseded
2	10/12/20	Policy reviewed by GMPS – No substantive change recommended. Noted by GMPS that an email address included under item 3.9 for people to make a complaint to Metro about privacy issues has been decommissioned. ICT were requested to reactivate the email address and route any incoming emails to the People and Safety Services Helpdesk. Endorsed by ELT on 16/03/21 and approved by Board on 31/03/21.	Superseded
3	13/07/21	Privacy Officer identified as General Manager Corporate Services. Hyperlink to Metro referenced document added.	Superseded
4	29/03/22	Review date extended to end of June 2022 to allow GMCS & Policy and Records Management Officer to complete document management reviews with departments in April 2022.	Superseded
5	31/05/22	Review date extended by one month to accommodate GMCS annual leave.	Current