PRIVACY POLICY

DOCUMENT CONTROL TABLE

Document Owner:	Corporate Services	**Section:**	Corporate Services
Endorsed by:	General Manager Corporate Services	**Date:**	1 April 2025
Approved By:	Metro Board	**Date:**	N/A
Next Review Due:	1 April 2028		

1 POLICY STATEMENT

Metro Tasmania (Metro) is dedicated to safeguarding individual privacy in line with the *Personal Information Protection Act 2004 (TAS)* and the Australian Privacy Principles (APPs) set forth in the *Privacy Act 1988 (CTH).* These principles govern the collection, use, and disclosure of personal information to ensure its confidentiality. For more information, visit http://www.oaic.gov.au/privacy.

Metro values the privacy rights of individuals and adheres to both Commonwealth and State laws concerning the collection and management of personal information. Personal information refers to any data or opinions about an individual that can identify them, such as their name, address, phone number, or email.

Our objective is to collect only the personal information necessary to fulfil our business requirements and comply with relevant regulations.

This policy explains how Metro gathers, handles, and manages personal information in accordance with these principles. It also provides an overview of the types of personal information we hold and how it is collected, used, and disclosed.

2 SCOPE

This policy applies to all Metro employees, Directors, contractors, volunteers and customers.

3 TYPE OF INFORMATION COLLECTED

3.1 PERSONAL INFORMATION

Customer Information

Metro may collect and store the following types of personal information related to customers:

- Transaction records from visits and logins to our Greencard website;
- Identification details such as name, date of birth, postal address, fax number, telephone number, email address, and pensioner or concession status;
- Complaint details;
- CCTV footage; and
- Any additional information deemed reasonably necessary.

Employee and Volunteer Information

Metro may collect and store the following types of personal information related to employees and volunteers:

- Identification details such as name, date of birth, postal address, fax number, telephone number, tax file number, bank account details, driver's license information, and superannuation fund details;
- Employment information;
- Income details;
- Complaint details; and
- Any additional information deemed reasonably necessary.

Contractor Information

Metro may collect and store the following types of personal information related to contractors:

- Identification details such as name, date of birth, postal address, fax number, telephone number, tax file number, bank account details, driver's license information, and any other licensing details; and
- Any additional information deemed reasonably necessary.

3.2 SENSITIVE INFORMATION

Sensitive Information Collection

We may need to collect sensitive information about you. Unless required or authorized by law, we will only collect this information with your consent.

Customer Sensitive Information

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

- Bank account details;
- Date of birth; and
- Centrelink concession details.

Employee Sensitive Information

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

- Health information;
- Criminal records;
- Bank account details; and
- Personal address.

3.3 INFORMATION REQUIRED BY LAW

We may collect information about you if it is required or authorised by law, or by a court or tribunal order.

4 COLLECTING INFORMATION

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

- To provide services to you;
- To respond to complaints;
- To manage and address potential legal actions, including dispute resolution;
- To protect the health and safety of our customers and employees;
- To manage accounts;
- To manage human resources;
- To identify you;
- To comply with applicable laws, regulations, or codes of practice; and

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

Where reasonable and practicable, we will collect personal information directly from you. This may occur when:

- You provide information over the telephone;
- You interact with us electronically or in person;
- You access our website;
- We provide services to you; and
- You complete a Greencard application form.

If you do not provide your personal information, we may be unable to:

- Provide the services you request; and
- Verify your identity.

5 COLLECTING PERSONAL INFORMATION FROM OTHER SOURCES

We may collect personal information about you from other sources when necessary. This may occur when:

- You have consented to the collection of the information from another party;
- We are required or authorised by law to collect the information from another party; and
- It is unreasonable or impracticable to collect the information directly from you.

Examples of other sources from which we may collect personal information include:

For Employees:

- Family members;
- Medical advisors;
- Current and former employers;
- Medicare;
- Centrelink;
- The Australian Tax Office;
- Government departments and agencies;
- Insurance companies and their authorised representatives; and
- Banks and financial institutions.

For Customers:

- Banks and financial institutions;
- Insurance companies; and
- Authorised professional advisors.

For both customers and employees, we may also access publicly available information from sources such as the electoral roll, telephone directories, or websites.

6 UNSOLICITED PERSONAL INFORMATION

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

7 USING THE INFORMATION

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

- You have consented to the use or disclosure for another purpose;
- You would reasonably expect us to use or disclose the information for another purpose;
- The use or disclosure is permitted under the *Privacy Act 1988 (CTH)* or the *Personal Information Protection Act 2004 (TAS);*
- The passing of database information to software vendors responsible for maintaining the software; and
- We are required by law to disclose the information.

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 the disclosure is directly related to protecting the health and safety of our employees or customers.

We are unlikely to disclose your personal information to any overseas recipients.

When we disclose your personal information, we will ensure that it is used, held, and disclosed in accordance with the *Privacy Act 1988 (CTH)* and other applicable laws.

8 QUALITY OF INFORMATION

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

If you believe that your personal information is inaccurate, incomplete, outdated, or irrelevant, please contact our Privacy Officer (General Manager Corporate Services) as outlined in Section 13 of this policy.

9 SECURITY OF INFORMATION

We store your personal information in various forms, including paper and electronic formats. We treat all personal information as confidential and take reasonable steps to protect it from:

- Misuse, interference, and loss; and
- Unauthorised access, modification, and disclosure.

Some of the methods we use to protect your personal information include:

- Limiting access to personal information to those who need it for their role;

- Taking measures to prevent third parties (including unauthorised members of the organisation) from overhearing or accessing the information;
- Using electronic security systems such as firewalls, data encryption, user identifiers, passwords, antivirus software, antispyware, and backup/recovery systems; and
- Controlling access to Metro buildings.

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

- The information is part of a Commonwealth record; and
- We are required by law or court/tribunal order to retain it.

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

10 ACCESS TO INFORMATION

You can access your personal information unless an exception under the *Privacy Act 1988 (CTH)* or the *Personal Information Protection Act 2004 (TAS)* applies. Exceptions may include situations where:

- Giving access would have an unreasonable impact on the privacy of others;
- The request is frivolous or vexatious; and/or
- The information relates to existing or anticipated legal proceedings and providing access may prejudice those proceedings or negotiations.

To request access to your personal information, please contact Metro's Privacy Officer in accordance with Section 13 of this policy.

Depending on the nature of your request, we may charge a small fee to cover the costs of providing access. We will inform you of any costs before processing your request.

We will respond to your access request within a reasonable timeframe (usually within 30 days) and provide access in the manner requested, if it is reasonable and practicable to do so.

11 CORRECTION OF INFORMATION

If you believe that any personal information we hold about you is incorrect, inaccurate, incomplete, out-of-date, irrelevant, or misleading, you can request that we correct it by contacting the Privacy Officer as outlined in Section 13 of this policy.

We will take reasonable steps to correct the information to ensure that, considering 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 request us to notify the other entity of the correction, we will take reasonable steps to do so, unless it is impractical or unlawful.

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

- Written reasons for the refusal, if it is reasonable to do so
- Information on the available mechanisms to challenge the refusal

We will respond to your correction request within a reasonable time, usually within 30 days.

12 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.

13 PRIVACY ISSUES

If you:

- Have any issues about the way we handle your personal information after reading this policy;
- Become aware of a potential breach of privacy; and/or
- Wish to make a complaint please contact our Privacy Officer as set out below:

  Privacy Officer
  Telephone: (03) 6233 4211
  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 is unable to resolve the matter, it will be escalated (internally or externally) as appropriate to facilitate resolution.

14 REPORTING ELIGIBLE DATA BREACHES

An eligible data breach occurs if:

- There is unauthorised access to or disclosure of your personal information, or information relating to you, that a reasonable person would conclude is likely to result in serious harm to you; or
- Your personal information or information relating to you is lost in circumstances where unauthorised access or disclosure is likely to occur, and it can be reasonably concluded that such an outcome would result in serious harm to you.

If we suspect an eligible data breach, we will conduct a reasonable and prompt assessment.

If we determine that an eligible data breach has occurred, we will notify you and the Office of the Australian Information Commissioner. Our notification will include:

- A description of what occurred;
- The types of information involved; and
- Recommended steps you should take in response to the breach.

15 EXTERNAL COMPLAINT MECHANISM

If you are not satisfied with the outcome of the Privacy Officer's investigation, or if we have not responded to you within a reasonable time, you can raise your concern with the Office of the Australian Information Commissioner (OAIC).

Complaints can be made to the OAIC in the following ways:

Office of the Australian Information Commissioner

- **Telephone**: 1300 363 992 (Mon-Thurs, 10:00am – 4:00pm AEST/AEDT)
- **Email**: FOI@oaic.gov.au

- **Mail**: GPO Box 5288, Sydney NSW 2001
- **Online**: OAIC Privacy Complaints

16 RESPONSIBILITIES

16.1 COMPLIANCE, MONITORING AND REVIEW

- The General Manager Corporate Services or their delegate is responsible for:
  i. Reviewing this policy according to its review cycle, or if changes to legislation, regulations, or government policies trigger a review;
  ii. Approving this policy if minimal or no amendments were made during the review; and/or
  iii. Seeking Executive Leadership Team endorsement if moderate to major amendments were made during the review, before seeking Board approval;
- The Board is responsible for approving this policy if moderate to major amendments were made.
- The Chief Executive Officer and Executive Leadership Team are responsible for the implementation and overseeing the compliance of this policy including effectively communicating privacy obligations to all employees.

16.2 REPORTING

Any material breaches of this policy will be reported to the Board through the Audit and Risk Committee, all other breaches will be reported to the CEO.

16.3 RECORDS MANAGEMENT

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

17 REVIEW PERIOD

This Policy will be reviewed every three years or earlier if required.

18 RELATED AND REFERENCED DOCUMENTS

18.1 METRO PROCEDURES

Code of Conduct Procedure
Data Management and Data Breach Procedure

18.2 LEGISLATION

Personal Information Protection Act 2004 (TAS)
Privacy Act 1988 (CTH)
Privacy Regulations 2013 (CTH)

19 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.	Superseded
6	20/02/23	Review conducted. Section 1 – Policy Statement and Contact details for Office of the Australian Information Commissioner in Section 14 – External Complaint Mechanism updated. Approved by Board on 01/03/23.	Superseded
7	01/04/25	Review conducted by GMCS. No content change required. Board approval not required.	Current