Policy No:	LOCAL POLICY 001
Subject/Title:	AFCS COMPLIANCE WITH PRIVACY PRINCIPLES
Issue Date:	08/04/2013
Date Reviewed:	31/03/2016

DEPARTMENT OF PLANNING, TRANSPORT AND INFRASTRUCTURE

COMPLIANCE WITH PRIVACY PRINCIPLES WHEN USING AFCS INFORMATION

1.0 Purpose

To ensure that people and organisations dealing with Adelaide Fare Collection System (AFCS) information comply with South Australian Privacy Principles.

2.0 Definitions

"Personal information" means information or an opinion, whether true or not, relating to **a natural person or the affairs of a natural person** whose identity is apparent, or can reasonably be ascertained, from the information or opinion. For the purpose of the AFCS this means information gathered as:

- part of Metrocard registration, forming a temporary or permanent customer record;
- part of payment or AutoRecharge functionality, forming a temporary or permanent customer record;
- validations and recharge data linked to a natural person.

The defined purposes for collection of personal information in the AFCS are:

- operation of the AFCS;
- registration of Metrocards;
- payment, refund and AutoRecharge processing;
- transport planning associated with analysing validations and sales.

3.0 Scope

South Australian Government Departments and public servants are subject to a privacy regime based on Information Privacy Principles which were contained in Premier and Cabinet Circular PC012 - Information Privacy Principles Instructions. The Information Privacy Principles cover the collection, storage, access, correction and disclosure of personal information held by the Department. All Departmental employees must ensure they handle personal information in accordance with these principles.

PC012 takes precedence over this specific policy. This policy specifically applies to all parties accessing AFCS information including staff, contractors, service providers and their agents, and other agencies.

4.0 Purpose

This policy ensures that all parties are aware of their responsibilities in relation to Privacy Principles as applied to the AFCS.

5.0 Collection of Personal Information

5.1 Right to Remain Anonymous

It is not obligatory for public transport users to provide personal information in order to use Metrocards or public transport services. Public transport users can choose to use anonymous Metrocards or buy anonymous Metrotickets.

5.2 Collection of Personal Information

Personal information will be collected lawfully and fairly and will not be collected unless it is necessary for the provision of public transport services including AFCS services. Personal information will only be retained for registered users. Registered users will have the ability to update personal information online or in person.

5.3 Personal Information to be Collected

Clause 13.0 contains details of the personal information that will be collected when a Metrocard is registered ("protect a Metrocard"), recharged or validated. Trip information – defined as the combination of origin and destination – is not collected, since the destination of the trip is not stored as passengers do not re-present the Metrocard at the time of alighting from the vehicle.

6.0 Storage

6.1 Secure storage

The AFCS is designed in accordance with Government security policies and systems, including the Information Security Management Framework (ISMF). Network and database security is a key design element. Databases are secured behind appropriate firewalls and logically and physically separated from other networks.

6.2 Access Controls

Access control is an inherent design component of the system. All access to databases and networks is subject to password protection. Most equipment access requires a secure employee pass with a PIN.

Users are assigned rights according to the level of access required to undertake their duties.

6.3 Audit Controls

Changes to Personal Information in a customer file creates an audit trail detailing the source and nature of the change.

7.0 Access and Correction

7.1 Customers accessing data

Customers are entitled to review their own personal information and request that it be amended for accuracy. Reasonable proof of identity is required before information is disclosed.

Requests for access to personal information of another person (eg a partner) should not be granted without the consent of that person. Customers may arrange for secure third party access to their accounts if required.

Where a parent or guardian requests access to personal information of a minor, reasonable proof of identity of the requestor is required in addition to reasonable proof of a relationship to the third party, before any information is disclosed.

7.2 Staff accessing data

Only staff with the correct authorisation are to access Personal Information. Staff must only access Personal Information for an authorised purpose. Normally this will only be on the request of the record-subject.

8.0 Use of Personal Information

8.1 Only use Personal Information for an Approved Purpose

Personal Information must not be used except for a purpose, or a purpose incidental to, a purpose for which AFCS data was collected.

8.2 Use of Validations data

The validations data will be used to provide registered users with a history of their transactions or to resolve disputes regarding the fare(s) deducted.

Validations data will not be used to establish an individual's pattern of validations without that user's express permission. The uses of personal information in the AFCS is described in Clause 13.0.

Validations data may be aggregated for the purpose of assessing service demand, service performance or to assist with public transport planning. Such aggregated data will not link to customer's personal information.

8.3 Permission to use Personal Information

The use of personal data for other purposes is only permitted if the customer has been asked and explicitly permits such use e.g. positively ticking a check box on the website.

8.4 Misuse

Misuse of Personal Information is prohibited. Personal Information must not be used for any "non-departmental" purpose.

9.0 Disclosure

9.1 Confidentiality

Personal Information must remain confidential and is not to be disclosed either within the Department of Planning, Transport and Infrastructure (DPTI) or to other parties unless provided for under this policy.

Confirmatory acknowledgement of personal details, for example a yes or no answer to a question concerning Personal Information such as "does this person live at this address", is also regarded as Personal Information and must not be disclosed.

9.2 Authorised Disclosure of Personal Information

Authorised disclosure of Personal Information may be required for law enforcement purposes. Disclosure may occur only after a written request from SAPOL is formally approved by an authorised officer of DPTI.

9.3 Contractors, service providers, and other third parties

Contractors, service providers, and other third parties - and their agents - who access, or have potential to access into the future, any personal information, must ensure compliance with this policy.

Contracts or agreements must contain specific clauses requiring compliance with this policy and relevant AFCS procedures. Where contractual arrangements do not exist, a separate enforceable arrangement may be entered into prior to any access being provided.

9.4 Management of extracted information

Personal information extracted from the AFCS whether in electronic or other form must be protected from accidental disclosure.

9.5 Reporting of Breaches or Incidents

Actual or suspected breaches of this policy must be reported as soon as practicable to the Administrative Assistant to Director, Public Transport Infrastructure.

Actual or suspected incidents where one party attempts to access the personal information of another party without appropriate authorisation must be reported as

soon as practicable to the Administrative Assistant to Director, Public Transport Infrastructure.

10.0 Complaints

Complaints in regard to the handling of Personal Information are subject to the same complaints handling process as all other complaints regarding public transport services. In the first instance customers may submit a complaint online, contact the InfoLine or attend an InfoCentre. Refer to adelaidemetro.com.au.

11.0 Notification of this Privacy Policy

11.1 Website Links

A link to this policy from the AdelaideMetro website will be enabled.

Links will also be enabled directly from relevant pages of the Metrocard sub-section of the Adelaide Metro website. This may also include 'plain language' versions of sections of this policy.

11.2 Staff Training

All staff who access, control, modify or use the Central System of the AFCS will be made aware of this policy during training. A record of such training will be maintained.

12.0 References

CABINET ADMINISTRATIVE INSTRUCTION 1/89,
ALSO KNOWN AS THE INFORMATION PRIVACY PRINCIPLES (IPPS) INSTRUCTION, AND PREMIER AND CABINET CIRCULAR 12, AS AMENDED BY CABINET 16 SEPTEMBER 2013
Cabinet Administrative Instruction No.1 of 1989
(Re-issued 30 July 1992, 18 May 2009, 4 February 2013, 5 August 2013 and 16 September 2013)

13.0 Schedule One: Personal Information Collected

13.1 During Registration ("Protect a Metrocard")

- Title
- First Name
- Surname
- Date of Birth (never re-presented again after registration)
- Street Address
- Suburb
- State
- Post Code
- Phone Number
- Second Phone Number
- Metrocard Unique Number(s)
- Seniors Card Number (Seniors Only)

and for customers who wish to access their account via the internet:

- Email address (this becomes their login to the system)
- Password (not visible to anyone)

13.2 Data stored on the Metrocard upon occurrence of a Validation

- Mode of transport: (bus, gate, tram, railcar)
- Boarding type: (first boarding, transfer)
- Stop ID: an internal database index number

- RouteID: an internal database index number
- Vehicle ID
- Fare product: a number from 1 to 8 indicating which fare type
- Date
- Time
- Service status
- Amount of value on fare product before validation
- Amount of value remaining on fare product after validation
- Amount of the operation (ie the fare or trip deducted)

There is no personal information stored on the Metrocard.

The purpose of putting this information on the Metrocard is to allow:

- an Inspector to check that the Metrocard (or magnetic ticket) has been validated.
- the on-board equipment to determine if the card should be allowed to transfer or another fare should be deducted.
- the customer to have evidence of the trips taken in case of a dispute over a fare.

13.3 Data Transferred to the Central System

The following Metrocard validation related data is transmitted from the Validation Equipment to the central system at "end of shift" (ie it is not transmitted in real time, there could be a number of hours between a validation and end-of-shift):

- Mode of transport: (bus, gate, tram, railcar)
- Boarding type: (first boarding, transfer)
- Stop ID: an internal database index number
- RouteID: an internal database index number
- Vehicle ID
- Type of media: Metrocard or Magnetic ticket
- Metrocard Unique Number (Magnetic tickets have no unique number)
- Fare product: a number from 1 to 8 indicating which fare type
- Fare product unique identifier
- Date
- Time
- Service status
- Amount of value on fare product before validation
- Amount of value remaining on fare product after validation
- Amount of the operation (ie the fare or trip deducted)
- GPS Location
- There is an internal index on the central system that converts the StopIDs and RouteIDs into data meaningful to DPTI. Only the origin of the trip is sent to the central system, there is no information about the trip destination because the passenger does not use the Metrocard on exiting.
- The primary purpose of retrieving this data is to: ensure that revenue is being collected; identify attempts at fraudulent activities; monitor that customers' balances are correct; generate patronage data to allow performance to be measured; allow historical patronage comparisons to be made for reporting purposes; and to determine where demand is greatest.

13.4 Protecting Metrocards

In the Central System a customer can opt to 'Protect' their Metrocard by providing some personal details. This associates the unique Metrocard number with their customer file. In return, if the card is lost or stolen, any balance remaining can be transferred to a replacement Metrocard and the original Metrocard can be cancelled. The same process of protecting a Metrocard provides customers with access to a

validation and recharge history for that Metrocard. Customers can opt not to 'protect' their Metrocard, in which case the Metrocard and customer remain anonymous. Alternatively, customers can opt to purchase a magnetic ticket, which is inherently anonymous.

13.5 Financial transactions

When a Metrocard is recharged the following information is sent to the central system

- Equipment ID
- Metrocard Unique Number
- Fare product: a number indicating which fare type
- Fare product unique identifier
- Date
- Time
- Amount of value on fare product before recharging
- Amount of value remaining on fare product after recharging
- Amount of the operation (ie the amount recharged)

The AFCS does not store any Credit Card or Debit Card information. Such information is securely stored in Bizgate (the SA Government payment gateway) during Internet transactions or for autoRecharge registration or sent directly to the card holder's card provider during Point of Sale transactions. Bizgate's policies can be found on the Service SA website.