FINANCIAL TRANSACTION CARDS POLICY AND PROCEDURE

Responsible Officer	Executive Manager: Community Engagement.
Approved by	Chairman
Review by	Executive Manager: Community Engagement
Last Reviewed	12/07/2015
Next Reviewed	31 /01/2017
Approved and commenced	12/07/2015

INTRODUCTION

The use of financial transaction cards, including credit cards, is a major convenience for Community Veracity and for employees/volunteers, and can, if properly managed, contribute to easier and more secure accounting of expenses. To achieve these benefits a number of precautionary procedures should be put in place.

PURPOSE

The purpose of this policy is to:

- ensure that organisational transactions are carried out as efficiently as possible through the use of credit cards and transaction cards as appropriate.
- guard against any possible abuse of organisational transaction cards.

POLICY

Transaction cards issued to Community Veracity, including those held in the name of any staff, volunteers or officers on behalf of the organisation, will only be used for those activities that are a direct consequence of the cardholders' function within the organisation. Their use will be monitored according to the procedures listed below. Any use of the card inconsistent with this policy and these procedures will be grounds for dismissal.

RESPONSIBILITIES

It is the responsibility of the Executive Manager: Community Engagement to ensure that:

- staff and volunteers are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately.

It is the responsibility of the all employees and volunteers to ensure that their usage of credit cards conforms to this policy.

PROCESSES

1. Card Issue

Any organisational financial transaction cards may only be issued by a board member, staff member, or volunteer where their functions and duties would be enhanced by their use. Cards will thus be issued only to people on the approved Organisational Financial Transaction Card List. The list shall be held by the Executive Manager: Community Engagement.

Other persons may be added to the list by the Board. The Board may delegate the power to add persons to the list to any or all of:

- The Finance Committee;
- The CEO;
- The auditor.

Cards may be issued on a temporary basis and recovered afterwards.

Each financial transaction card will be issued to a specific person, who will remain personally accountable for the use of the card. Cardholders will sign a declaration to this effect.

Only the authorised signatory may use the card. No more than one card shall be issued per cardholder. Credit limits as appropriate shall be set for each card by the issuing authority.

2. Cardholder's Responsibilities

The Cardholder shall:

- In all cases obtain and retain sufficient supporting documentation to validate the expense (e.g. tax invoice) or shall in lieu provide a statutory declaration.
- Attach supporting documentation to the monthly statement from the bank.
- Review the monthly statement for inaccuracies (and report these to the Executive Manager: Community Engagement).
- Verify that that goods and services listed were received.
- Sign the monthly statement to verify that transactions have been made for official purposes.
- Forward the papers to the authorised signatory for approval (the Board Chair shall authorise payments to the Executive Manager: Community Engagement; the Executive Manager: Community Engagement shall authorise the expenditure of all other cardholders).
- Notify the bank and the Executive Manager: Community Engagement (or in the case of the Executive Manager: Community Engagement, the Board Chair) immediately if
    - The card is lost or stolen; and/or
    - Any unauthorised transaction is detected or suspected.

- Notify the Executive Manager: Community Engagement and the bank of any change in name or contact details.
- Take adequate measures to ensure the security of the card.
- Return the card to the Executive Manager: Community Engagement if
    - The cardholder resigns;
    - the Executive Manager: Community Engagement determines that there is no longer a need for the cardholder to retain his or her card; or
    - the card has been cancelled by the bank.
- Be personally liable for any unauthorised transaction unless the card is lost, stolen or subject to fraud on some part of a third party.

The Cardholder shall not:

- exceed any maximum limits set for the card from time to time.
- obtain cash advances through the card.
- use the card for any proscribed purchases.
- authorise their own expenditure.
- claim double allowances (i.e. request reimbursement for an expense already paid by the card).

3. Card Expenditure

The card will only be used for those activities that are a direct consequence of the cardholders' function within the organisation.

Where coincident and/or private expenditure occurs on the same transaction (where, for example, a person incurs a debt for personal telephone calls during a hotel stay) the cardholder must settle the private expense prior to charging the balance on the organisational card.

Where doubt exists as to whether or not an item is function-related, prior authorisation should be obtained from the CEO (or, in the case of the CEO's own card, the Chair of the Board or the person of the Finance Committee).

The use of the corporate card for "services of a dubious nature" is expressly prohibited. "Services of a dubious nature" are defined as any goods or services that might bring the name of the organisation into disrepute.

4. Card Misconduct

Wherever a breach in this policy occurs, the CEO must assess the nature of the breach and institute an appropriate disciplinary process, including (without limitation of the Community Veracity's right to summarily dismiss an employee for serious misconduct):

- counselling and / or verbal warning (and diary or file note created and retained on employee's personnel file); and
- a written warning.

The CEO may determine whether to report a breach of the policy to the police for criminal investigation.

At the next Finance Committee meeting the CEO shall report:

- the investigation of the circumstances of the breach;
- police reports and action (if any); and
- disciplinary action taken (if any).