Payment Card Compliance Policy

20 November 2023

#### City of Port Phillip logo

#### City of Port Phillip

99a Carlisle Street

St Kilda VIC 3182

Phone: ASSIST 03 9209 6777

Email: [portphillip.vic.gov.au/contact-us](mailto:portphillip.vic.gov.au/contact-us)

Website: [portphillip.vic.gov.au](https://www.portphillip.vic.gov.au/)

##### Divercity

Receive the latest news from your City and Council [portphillip.vic.gov.au/divercity](https://www.portphillip.vic.gov.au/about-the-council/divercity-enews-and-local-media)



##### National Relay Service

If you are deaf or have a hearing or speech impairment, you can phone us through the National Relay Service (NRS):

TTY users, dial 133677, ask for 03 9209 6777

Voice Relay users, phone 1300 555 727,

then ask for 03 9209 6777.

[relayservice.gov.au](https://www.infrastructure.gov.au/media-communications-arts/phone/services-people-disability/accesshub" \o "relayservice.gov.au)



## Policy

Responsible Service / Department:

Financial Accounting/ Finance

Adoption authorised:

ELT

Date of adoption:

20 November 2023

Date effective from:

20 November 2023

Document Set ID (ECM):

[Insert Text]

Subject (Index name in ECM):

[Insert Text]

Endorsed CEO or ELT member or department manager to make and approve document editorial amendments:

Chief Financial Officer

Annual desktop review date:

September

Review date:

November 2025

Completion date:

November 2027

Version number:

1

Stakeholder review and engagement:

N/A

Relevant Legislation:

N/A

Associated Strategic Direction #:

5 Well Governed Port Phillip

Associated instruments:

Payment Card Procedures

Supersedes:

Payment Card Policy 2019

Contents

[Policy 3](#_Toc149483847)

[Purpose 6](#_Toc149483848)

[Scope 6](#_Toc149483849)

[Definitions 7](#_Toc149483850)

[Responsibilities 9](#_Toc149483851)

[Financial Accounting Team 9](#_Toc149483852)

[Head Financial Accounting & Services 9](#_Toc149483853)

[Chief Financial Officer 9](#_Toc149483854)

[Digital Technology Services 9](#_Toc149483855)

[Cashiering staff (all locations) 10](#_Toc149483856)

[PCI Compliance Team 10](#_Toc149483857)

[*.* PCI DSS 11](#_Toc149483858)

[Card Acceptance and Approval 11](#_Toc149483859)

[Implementation of Payment Card Processing 11](#_Toc149483860)

[Training 12](#_Toc149483861)

[Acceptable Payment Card Format 12](#_Toc149483862)

[Non-accepted payment card format 12](#_Toc149483863)

[Payment Processing Requirements 12](#_Toc149483864)

[Data Retention 13](#_Toc149483865)

[Disposal of Data 13](#_Toc149483866)

[Compliance Monitoring 14](#_Toc149483867)

[Relevant Policy, Regulations or Legislation 14](#_Toc149483868)

# Purpose

This document details the measures in place for Council to ensure the prevention of loss or disclosure of sensitive customer information, specifically payment card data. The failure to protect customer information may result in the following:

* Financial loss for customers,
* Suspension of credit card processing privileges for the organisation,
* Damage to the reputation of the Council and
* Fines imposed due to failure to comply with the Payment Card Industry Data Security Standards (PCI DSS).

# Scope

The City of Port Phillip Payment Card Compliance Policy applies to all staff, organisations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Council.

City of Port Phillip to allows acceptance of payment cards as a form of payment for goods and services. Council requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the City of Port Phillip payment card procedures, and other supporting documents.

# Definitions

|  |  |
| --- | --- |
| Term | Definition |
| Cardholder | Someone who owns and benefits from the use of a membership card, particularly a credit card. |
| Card Holder Data (CHD) | Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date, and the Service Code. |
| Cardholder Name | The name of the Cardholder to whom the card has been issued. |
| CAV2, CVC2, CID, or CVV2 CCV data | The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions. |
| CBA | Commonwealth Bank of Australia |
| DTS | Digital & Technology Services Department |
| ERP System | Enterprise Resource Planning System- One Council |
| Expiration Date | The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card. |
| Magnetic Stripe (i.e., track) data | Data encoded in the magnetic stripe or equivalent data on a chip used for authorisation during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorisation. |
| Merchant Department | Any department or unit (can be a group of departments or a subset of a department) which has been approved by the Finance department to accept credit cards and has been assigned a Merchant identification number. |
| Payment Cards | The following cards are accepted at the city of Port Phillip:   * Mastercard and Visa Credit * Mastercard and Visa Debit * American Express (Amex) * Eftpos/Debit Card |
| Term | **Definition** |
| Payment Card Industry Data Security Standards (PCI DSS) | The security requirements defined by the Payment Card Industry Security Standards Council and the major Credit Card Brands: Visa, MasterCard and American Express. |
| PIN/PIN block | Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message. |
| Primary Account Number (PAN) | Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip.  PAN identifies the issuer of the card and the account and includes a check digit as an authentication device. |
| Sensitive Authentication Data | Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, CCV or CVV2 data and PIN/PIN block. |
| Service Code | The service code that permits where the card is used and for what. This is also known as the MCC- merchant category code |

# Responsibilities

## Financial Accounting Team

Responsible for:

* Ownership and issuing the Payment Card Compliance Policy and a Payment Card Procedures
* Reviewing and processing requests from business units to accept payments by card.
* Administering and monitoring business units to ensure their understanding of their responsibilities.
* Maintains the register of Eftpos terminals for tracking.
* Liaising with Council’s operational banker
* Requesting and issuing payment processing equipment to business units
* Reconciliation and receipt of payments received into Councils bank account.

## Head Financial Accounting & Services

Responsible for:

* Ensuring the policy and procedures are regularly reviewed and updated (where required) on an annual basis.
* Reviewing and approving requests from business units to accept payments by card.
* Completing the annual Self- Assessment Questionnaire to attest to Councils PCI Compliance and obtain certification (Annual Merchant Survey Renewal)
* Coordinating the annual CampusGuard audit and ensuring recommendations are implemented.

## Chief Financial Officer

Responsible for:

* Final approval of requests from business units to accept payments by card.
* Review and approval of any exceptions to this policy eg alternate payment equipment requests

## Digital Technology Services

Responsible for:

* Reviewing requests from business for external websites to accept card payment.
* Approving these in conjunction with Finance
* Liaising with Finance on all payment channels and payment requests

## Cashiering staff (all locations)

Responsible for:

* Adhering to the Payment Card Compliance Policy and Payment Card Procedures in the course of their work
* Undertaking the mandatory training as required.
* This includes but is not limited to staff accepting payment at the following.
  + Assist front counter (all Town Halls)
  + South Melbourne Town Hall
  + Child Care Centre staff
  + Operations Centre (transfer station)

**CampusGuard**

Council contract with an external partner to advise and monitor our compliance status through the Procurement Australia Panel.

Campus Guard are responsible for

* Meeting with the PCI team monthly
* Advising on any matters raised to provide compliant solutions.
* Conducting annual audit reviews of all payment processes and providing recommendations to maintain compliance.
* Reviewing council websites and payment channels to advise on corrective action to address risk.

## PCI Compliance Team

Responsible for:

* Compliance monitoring
* Management of Councils PCI DSS compliant status
* Enact any new processes required to ensure PCI compliance status is maintained.

The PCI Compliance team includes CampusGuard, our external advisor on all PCI matters and the following representatives from Council:

* + Head of Financial Accounting & Services
  + Senior Financial Accountant
  + Financial Accountant
  + ICT Governance and Risk Officer
  + Risk & Compliance Advisor

# *.* PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the major credit card companies including VISA, MasterCard and American Express. These security requirements apply to all transactions surrounding the payment card industry and the merchants/ organisations that accept these cards as forms of payment.

To accept credit card payments, City of Port Phillip must prove and maintain compliance with the Payment Card Industry Data Security Standards. City of Port Phillip’s Payment Card Compliance Policy and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done to reduce the organisational risk associated with the administration of credit card payments by individual departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

## Card Acceptance and Approval

All business units that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by Finance.

All merchants (business units) should submit their requests through ServiceNow to the Finance team where they will be provided with a questionnaire to be completed before the request can be processed.

All business units who wish to take payments via payment cards must be approved by the Head of Financial Accounting and Services who will forward the request should be forwarded to the Chief Financial Officer for final approval before implementation.

### Implementation of Payment Card Processing

Business units accepting payment cards must be approved by Finance/ the Financial Accounting Team and ensure adherence to this policy and supporting documents and the Payment Card Industry Data Security Standard and institutional Data Security Policies that must be followed.

Business units must accept only authorised payment cards and agree to operate in accordance with the contracts the Council holds with its service providers.

Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

### Training

All staff responsible for the handling of credit card information and payment card data must complete mandatory PCI DSS training as detailed in the Payment Card Procedures. Business units will be unable to process payments if staff training is not completed or up to date.

### Acceptable Payment Card Format

Payment card information can only be received via the following channels:

* **In person**- for processing on an approved Commonwealth Bank Eftpos terminal, as allocated by the Financial Accounting Team. All Eftpos terminals must be included on a register that is maintained by Finance.
* **Online**- through approved CoPP websites that comply with PCI DSS requirements which have been pre-approved by Finance- in consultation with Digital Technology Services. e.g. e-Services, My Port Phillip, St Kilda Festival, South Melbourne Market, BPoint.
* **Over the phone**- through BPoint IVR (Interactive Voice Recognition) – available for OneCouncil debtor accounts (property and rating)
* **Card not present**- where a payment is processed directly onto an Eftpos terminal using card number information provided by a customer on the telephone while the customer waits. Also known as MOTO (Mail Order/Telephone Order).

### Non-accepted payment card format

* Cardholder information received on mailed in forms are not accepted. Any links to these on any Council websites will be removed. Refer to Payment Card Guidelines for the procedures on processing these payments.
* Cardholder data (CHD) received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. See below for the appropriate method of responding to and securely destroying the cardholder data.

### Payment Processing Requirements

All processing equipment must be obtained through the Financial Accounting Team (Helpdesk- Finance) and integrate with Councils operational banking provider (CBA).

Exceptions to this policy will be limited and will require a business plan (including reason why the available central processing systems will not work for your area) to be submitted and approved by the Chief Financial Officer and the Chief Information and Innovation Officer (DTS) in advance of any equipment or system purchase.

All payments received must be directed into a CBA approved bank account. The type and nature of the electronic transaction will dictate where the transaction will be deposited and is managed by the Financial Accounting Team.

Accounting entries to record the receipt of the payment will be integrated directly into the Council’s Financial System, whenever possible, to ensure timely recording of transactions and expedite the prompt reconcilement of general ledger and bank accounts.

## Data Retention

As a rule, cardholder data storage should be kept to a minimum to reduce risk. The following rules apply for the storage and retention of cardholder data:

* Data storage amount and retention time should not exceed 12 months.
* All paperwork containing credit card information that is to be retained must only display the truncated card number. The maximum number of digits that can be displayed to mask the customer PAN (Primary Account Number) is the first 6 and last 4 digits of the card number e.g. 5163 22XX XXXX 1234.
* All Eftpos terminal receipts only print out the truncated number to comply with PCI DSS requirements.
* Scanned documents containing cardholder information are to be stored in secure folders within Record Manager with the PAN truncated as above and access restricted to staff within the relevant business unit as required.
* Paper documents must be kept in a secure location within the business unit, with access restricted to staff with a need to know \*Note that provided the cardholder information and PAN is correctly masked, the retention of this paperwork is compliant with PCI DSS standards.
* All data will be treated as confidential.
* Files stored on the network containing card numbers and information are required to be encrypted and password protected with network scans conducted on a quarterly basis to identify those which are not secure for this to be rectified immediately. Refer to the ICT Security Policy.

## Disposal of Data

Data that is not necessary to conduct business will not be retained in any format.

* Cardholder data that is securely stored on the network will be deleted in accordance with the relevant retention and disposal schedule and the Information Security Policy**.**
* Cardholder data that is correctly truncated and stored on Content Manager will be deleted accordance with the relevant retention and disposal schedule within Content Manager.
* Hard copy physical data is to be securely shredded after 12 months.

# Compliance Monitoring

The PCI Compliance Team has been established with representation from Finance, Digital and Technology Services, Risk & Assurance and CampusGuard

The team meet monthly or earlier if issues arise.

Standard items will be discussed and addressed by the team as follows:

* Breaches and issues reported to the team
* Review of PCI statistics and tracking
* Monitoring of training registers

# Relevant Policy, Regulations or Legislation

* Payment Card Industry Data Security Standards (PCI DSS)
* Payment Card Guidelines November 2023
* ICT Policies
* Privacy Policy
* Annual Merchant Survey Renewal