www.rbwm.gov.uk Royal Borough of Windsor & Maidenhead

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

SECURITY POLICY

Processing Electronic Card Payments

Introduction and Policy Aim
The Payment Card Industry Data Security Standard (PCI-DSS) is a worldwide information security standard, created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. It applies to all organisations that receive, process, store and pass cardholder information.

The Royal Borough of Windsor and Maidenhead (the council) is liable to fines from its merchant bank should it fail to comply with PCI-DSS.

This policy is required to ensure compliance with Point 9 and 12 of the PCI-DSS Standard.

Policy Statement
All card processing activities of the council will comply with the PCI-DSS industry standard. No activity or technology may obstruct compliance with the PCI DSS.

Not covered by this Policy
The council does not accept some cards: American Express, Diners Club, JCB

Those Affected by the Policy
Anyone performing council duties or providing council services facilitating card payments. It applies to Councillors; other organisations conducting council business; employees; contractual third parties and agents of the council.

Roles and Responsibilities
1. Council Operational support workers – must understand and comply with the policy.
2. Council Managers and Team Leaders – must ensure their staff understand the policy and are aware of their obligation to comply with it.
3. Senior Systems Accountant – must ensure relevant card payment security training is carried out and that staff comply with this policy.
4. The IT Service – must manage IT Services and Infrastructure in accordance with the requirements of PCI DSS.

Services must comply with this policy to minimise the risk to both customers and the council. Failure to comply will render the council liable for fines and may also result in Visa and/or MasterCard preventing transactions from being processed.

Policy Compliance
This policy is mandatory for all staff. Failure to comply with this procedure may result in disciplinary or other action. Heads of Service are responsible for ensuring that their staff are aware of the policy and that it is complied with.

If you do not understand this policy, or how it may apply to you, get advice from your council manager, or from the Senior Systems Accountant on 01628 796923.

Alternatively email Tanith.Champion@rbwm.gov.uk

Other actions will be taken to encourage compliance, namely:

1. The council submits an annual Self-Assessment Questionnaire (SAQ) to prove compliancy.

2. The council will contractually require all third parties with access to cardholder data to adhere to PCI-DSS requirements. These contracts will clearly define information security responsibilities for contractors.

3. Ad hoc checks will take place to ensure employees are maintaining PCI-DSS security procedures.

4. Annual compliancy confirmation will be sought from all staff processing electronic card payments.

Applying the Policy – Security Breaches

In the event of there being a security breach of data, Staff must contact the appropriate member of Staff – See Point 8. The member of staff must then contact parties listed below and ensure that card processing is discontinued immediately.

- Elavon Customer Services 0845 8500195
- Lloyds (PDQ terminals) Customer Services 01628 567100
  email cnethelp@firstdatacorp.co.uk

Staff must also submit an internal council security incident report.

Applying the Policy - Corporate Card Payment Systems

The council has a corporate electronic card payments system which allows various types of income to be paid using a number of means as listed below:

- Online
- Telephone
- Automated Telephone Line
- Kiosk (card and cash)

Online Processing

- In the first instance customers should make payment for goods and services online using the Pay Online link on the council website, however only certain payments are set up to pay using this method. This is the preferred method and best practice for taking payments.

On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer. This is the only Finance confirmation document that will be received by the customer for the payment.

If a customer's payment has been unsuccessful or declined, the customer in the first instance should contact their card provider. The most common reason for a declined transaction is the card provider suspecting the transaction may be fraudulent.

If a customer faces difficulty in making a payment then they can email Epaymemts@rbwm.gov.uk for assistance or contact the Customer Contact Centre

where an agent will answer queries and can take the payment over the telephone.

Telephone Processing

Various payments can be taken over the telephone by either a Customer Contact Centre agent or specific service officer. Card details must never be written down by any member of staff for a future payment attempt. For all card details which are processed through the corporate payments system, no card details are retained by the authority.

There is no internal council access to full card details as this information is not stored within the council's IT network.

Applying the Policy - Card Payment Terminals (PDQ machines)

There are specific services that use PDQ terminals and not the Corporate Payments System. Where these terminals are used the following procedures apply.

1. Customer Present with a Card

When the customer is present the card should be processed through the PDQ machine according to the machine instructions.

1.1 If the transaction is successfully processed, the merchant copy should be stored securely (see Storage of Card Details) and the customer copy given to the customer.

1.2 If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely (see Storage of Card Details).

2. By Telephone

Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time and must not be written down or noted anywhere.

2.1 When card details are being provided in a telephone call these must not be repeated back to the customer in such a way as to be audible to third parties.

2.2 If it is not possible to submit the card details immediately then a call back must be requested or offered. Please refer to Section 2 above 'By Telephone'.

3. Card Details Received In Writing

Some customers may provide their card payment information in writing for processing i.e. by fax, in a letter, email or by booking form. Customers should be deterred from providing the information in this manner as it is not secure. There is no guarantee that these details have not been intercepted prior to being received by the council.

3.1 When details have been received by this method they must be processed immediately upon receipt.

3.2 Once the payment has been successfully authorised, the original document showing the full card details must be cross cut shredded.

If the details have been received by email then the email must be deleted from the Inbox and the Deleted mail folder. If the email requires a response, the card

information provided should not be contained within the reply.

3.3 In a situation where it is not possible to process the transaction immediately then the details must be stored in a secure environment such as a locked drawer or cabinet. This is only to be actioned in exceptional circumstances.

3.4 For PDQ records, if the transaction is successfully processed, the merchant copy should be stored until transaction reconciliation complete.

3.5 If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be sent to the customer and the merchant copy should be stored within the till drawer or cash box for the duration of the working day. When storing merchant copy receipts these must be treated as a confidential document and should be marked accordingly.

Applying the Policy – Storage of Card Details

1. Storage of card details on computers in any format (e.g. email, Access databases, Excel spreadsheets, USB memory sticks) breaches the Security Standard Regulations.

If this occurs the result could be large monetary fines from Visa and MasterCard.
This is because there is risk of fraudsters obtaining card details by hacking into computers or storage media which stores cardholder information.

2. Merchant copies of PDQ receipts must be destroyed once transaction reconciliation complete.

Applying the Policy – Data Retention and Disposal

1. Services are responsible for complying with the council's 'Information Retention and Disposal Policy' which can be found on the council intranet.

2. Services retaining card data must carry out a review, at least quarterly, to remove data that exceeds requirements defined in the data retention policy.

3. Retained data should be securely disposed of by cross-cut shredding when no longer required.

Applying the Policy – Electronic Transfer of Data

1.It is strictly prohibited to transfer card data electronically both internally or externally to the council. This includes the use of end user messaging technologies.

Applying the Policy - Point of Sale(PoS) Card Devices

1. All devices in use must comply with PCI standards.

2. All devices are included in the council inventory which contains key data identified by the standard.

3. Devices must be periodically inspected to detect tampering or substitution.

4 Staff using such devices must be trained to be aware of attempted tampering or replacement of devices.

5. Services using such devices must take ownership of their use and adhere to the requirements listed above.

Applying the Policy – Refunds

1. Corporate Electronic Payments

Refunds can only be processed back to the originating card if
(a) the card is still valid and
(b) if the payment was made either online or via the telephone where customer information has been completed
(but not automated payment line or Kiosk card transactions).

The refund must be approved by the responsible Service Head via email then forwarded to the nominated person.

The corporate system is then accessed and the refund is processed back to the source card from which the original transaction was authorised. It is possible to process part refunds where necessary but the refund cannot exceed the original amount.

2. Other Payment Methods

Refunds for other payment methods have to be processed by completing Payment Request Form which is processed and paid via the Finance system (Agresso). This is because the original payment does not capture the cardholder's details to facilitate a refund.

Contacts

If you have any questions about the details in this policy, or have difficulty complying with any part of it, please contact one of the people below.

Senior Systems Accountant 01628 796923 email Tanith.Champion@rbwm.gov.uk
Deputy Director and Head of Finance 01628 796341 email Rob.Stubbs@rbwm.gov.uk
RBWM IT Service 01628 796000 email ICTSecurity@rbwm.gov.uk

Related Information

General information about PCI-DSS can be found at
https://www.pcisecuritystandards.org/security_standards/why_comply.php

Legal and Regulatory Obligations

UK Data Protection Act

Definitions

PCI DSS The Payment Card Industry Data Security Standards
PSP Payment Service Providers, i.e. Elavon (corporate systems), Lloyds (Cardnet Payments)
SAQ Self-Assessment Questionnaire
PDQ Process Data Quickly or Pretty Damn Quick
CVV Card Verification Value (3 digit code on back of card)
CVC Card Verification Code (3 digit code on back of card)
PoS Payment locations utilising PDQ card devices