MELKSHAM WITHOUT PARISH COUNCIL

Payment Card Security Policy and Procedures

Adherence to this policy and the associated procedures is mandatory for all staff who handle or process card payments on behalf of the Council.

Introduction

All businesses that handle card payment data are required to comply with industry rules aimed at increasing data security. These are set out in the Payment Card Industry Data Security Standards ("PCI DSS"), which were developed by the five card brands: VISA, MasterCard, AMEX, JCB and Discover. The purpose of PCI DSS is to ensure that businesses are reducing the risk of card payment data theft and fraud and therefore providing a secure environment for their customers to make payment. The standard applies to all organisations that hold, process, or exchange cardholder information. Enforcement of compliance is via the organisation's card provider. Organisations that fail to meet the compliance requirements risk losing their ability to process card payments and being audited and/or fined.

The Council's preferred method for taking individual payments for goods and services from Allotment Holders, hirers of the Sports Pavilion & Field facilities and other service users is on-line via Bank Transfer, via card payment, cheque or cash. Where staff use Point of Sale Terminals (PDQ or card machines) such machines must comply with the requirements.

For more information please refer to https://www.pcisecuritystandards.org/

Purposes of Policy

The purpose of this policy is to set out the requirements of the PCI DSS in respect of the transmission, processing and storage of cardholder data, and the key responsibilities in connection with the achievement and maintenance of compliance with PCI DSS. It applies to all individuals and systems within the Council that come into contact with cardholder data, whether these be electronic or paper based.

Definition of Cardholder Data

Cardholder data consists of 2 main sets of data that must be protected by the Council at all times. These include:

CARD PAYMENT DATA	
Cardholder Data	**Sensitive Authentication Data (SAD)**
Primary Account Number (PAN) i.e. the 16 digit number on the front of the card.	Full Magnetic Stripe Data/Chip Data
Cardholder Name	CAV2/CVC2/CVV2/CID i.e. the last 3 digits on the signature strip on the back of the card
Expiration Date	Pin Numbers
Service Code	

PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply**.**

Responsibility and internal control

The management and control of information received, in respect of cards at the Council, applies to all employees that handle card payment data and any other data that is associated to legislation e.g. Data Protection Act.

The following procedures must be adhered to:

Card Payment Policy

Access to payment card transactions and data must be restricted to only those members of staff who need access as part of their role.

Staff should be made aware of the importance and confidentiality of card payment data e.g. appropriate checks and mandatory training is undertaken prior to allowing access to card payment data.

It is strictly prohibited to **send, receive, process and store** card details by unapproved Council methods.

Merchant copies of payment receipts must be retained in a secure, locked cabinet or room at all times and shredded immediately after use.

Council Approved Card Payment Methods and Services

Card data must only be received and processed by the Council approved methods and services. These are:

When the customer is present the card should be processed through the PDQ/EPOS machine according to the machine's instructions. If the transaction is successfully processed, the merchant's copy should be securely stored and the customers copy should be given to the customer. If the transaction is declined, the customer should be advised immediately and the customer copy stating that the payment has been declined should be given to the customer with the merchant's copy being stored securely. The option of paying on another card should be offered.

When the customer is not present the Council will allow payments via telephone. Where card details are provided during a telephone call, these must be processed directly into the PDQ or online payment system at the time. The Card details **must not** be written down. When card details are being delivered via phone they must not be repeated back to the customer. If it is not possible for the card details to be submitted immediately then a call back must be offered.

Unapproved Card Payment Methods

The following are unapproved methods of payment and should not be used:

Post/Written

Email

Voicemail/Recordings

Accepting cardholder data via the above methods exposes the Council to non-compliance with the PCI-DSS. This may result in fines, reputational risk if there is a data breach and ultimately potential withdrawal of the facility to take payments by credit or debit cards.

Under no circumstances should the non-approved payment methods be used

In the event of receiving card payment data via an unapproved method the data should be disposed of securely once identified e.g. if an Allotment Holder emails card details the email should be deleted and the sender contacted to arrange payment by one of the approved methods.

Storage of Card Payment Data

In the event that storage is required for operational, regulative and legislative requirements,

ONLY the data below can be stored:

Primary Account number (PAN) – First 6 or last 4 digits only

Cardholder Name

Service Code

Expiration Date

The approved methods are designed to securely store the relevant data for legislative requirements.

Below are only a few examples of further controls required and must be active at all times with the appropriate technology in place:

Masking to ensure **ONLY the first 6 OR last 4 digits of the PAN** can be seen (relevant to displaying on computer screens/receipts/voicemail)

Truncation, hashing and encryption via transmission and storage databases

Segregation away from other data sources on a designated secure server

Technical hardening and further controls of all aspects of systems, network and services used to process/store/transmit card payment data
Technical vulnerability and penetration testing of services on a regular basis

Receipt Rolls

The customer copy must be returned directly to the customer. The merchant copy of the card terminal receipt roll must be stored securely in a locked location with access control or a log of access.

Refunds

All refunds must be returned using the original payment source and be made to the customer who made the original payment.

Where possible these should be returned to the card on which the original payment was made. The only permissible exception is where the card has expired or an account is closed. **Proof of this should be obtained**. In these circumstances' refunds may be made to an alternative card held by the payee.

Problems with Payment Card Transactions

If a customer's payment has been unsuccessful or declined, the customer in the first instance should contact their card provider.

Secure Disposal

All assets that have the capability of storing card payment details must be disposed of in a secure manner.

Incident Management

The Clerk is responsible for ensuring staff are aware of this policy, the associated procedures and that these are adhered to. Mandatory training is provided and should be undertaken annually by staff handling payment card transactions.

In the event that an information asset is damaged, lost, or compromised it must be reported immediately to the Clerk. If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to the Clerk and the PCI DSS Team (pcidss@lboro.ac.uk). They should feel able to do so in the case of genuine mistakes as well as if they are concerned about poor practice by others. The PCI DSS team in consultation with the Clerk and the Chair of the Staffing Committee will decide on whether a further investigation is required.
Individual staff who do not comply with the requirements of the training and this set of policies and procedures may be subject to disciplinary action.

For review and adoption at Full Council meeting 15th April 2019