DARTFORD BOROUGH COUNCIL

SECURITY POLICY – PROCESSING ELECTRONIC CARD PAYMENTS

1. **INTRODUCTION & POLICY AIM**

   As an organisation that processes payments by debit and credit cards, we must comply with a set of standards to ensure the security of card information. The standards are known as the Payment Card Industry Data Security Standard (PCI-DSS), a worldwide information security standard, managed and maintained by the Payment Card Industry Security Standards Council and created to help organisations that process card payments, prevent card fraud through increased controls around data and its exposure to compromisation. It applies to all organisations that receive, process, store and pass cardholder information.

   The Council handles cardholder information on a daily basis. It must therefore have adequate safeguards in place to protect cardholder privacy, to maintain a secure environment in which to process cardholder information and to ensure compliance with PCI-DSS. We will however, limit exposure to risks by using industry standard PCI-DSS compliant software and systems, rather than creating bespoke Council systems.

2. **POLICY STATEMENT** - All card processing activities will comply with the PCI-DSS. It is essential that no activity or technology obstructs compliance with the PCI-DSS.

3. **NOT COVERED BY THIS POLICY** - The Council does not accept American Express, Diners Club and Japanese Credit Bank cards.

4. **COMPLIANCE WITH THIS POLICY**

   The Customer Service Manager must be consulted before starting any process and particularly any procurement process, involving card payments. A Data Protection Impact Assessment, must be completed, in consultation with the Data Protection Officer.

   In order to minimise the risks to both customers and the Council, all staff who facilitate card payments, for Council services, must comply with this Policy. Failure to comply may make the Council liable to fines and may also result in card providers preventing transactions from being processed.

   Failure by staff to comply with this Policy, may result in disciplinary proceedings.

   The following are implemented to ensure compliance with this Policy:

   1. the submission to Lloyds Cardnet Services , of an annual self-assessment questionnaire ;
   2. contractually requiring third parties who process cardholder data, to adhere to PCI-DSS;
   3. annual compliance confirmation from all staff processing electronic card payments.

5. **IDENTIFIED ROLES & RESPONSIBILITIES**

All personnel (employees, contractors, vendors and third parties) involved in the storage, transfer or processing of cardholder data or that can affect the security of the card holder data must abide by the relevant PCI - DSS policies and procedures (see Appendix 1).

6. **INTERACTION BETWEEN PCI - DSS & DATA PROTECTION LEGISLATION** (General Data Protection Regulation and the Data Protection Act 2018) - Personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information being processed, then that information may be personal data.

The PCI - DSS aims to help organisations process card payments securely and reduce card fraud. To achieve that, it implies strict security controls for storing, transmitting, and processing cardholder's data. The primary goal of implementing PCI - DSS is to protect the cardholder information. That also includes personal information as defined by data protection legislation.

Cardholder data refers to the card number across the centre of the card (otherwise known as the Primary Account Number, or PAN), the cardholder name, the expiry date and the service code (also known as the security code).

The PAN is the defining factor for cardholder data. If the cardholder name, service code, and/or expiry date are stored, processed or transmitted with the PAN, they must be protected in accordance with the PCI - DSS requirements. Storage of cardholder data is permitted, but the PAN must always be rendered unreadable.

Sensitive information is security-related information. This includes (but is not limited to) card validation codes, full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN blocks. This information is used to authenticate cardholders and/or authorise payment card transactions.

Under no circumstances can sensitive information be stored in any form.

7. **SECURITY BREACHES**- A data security breach must be reported to the Customer Service Manager, who in turn will contact:

- the Senior Information Risk Officer) SIRO;
- the Data Protection Officer (DPO); and
- Lloyds Cardnet Services – 0330 8080 798 or www.LLoydsBankCardnet.com

The Customer Service Manager will undertake and submit an internal security incident report to the SIRO and the DPO.

8. **APPLYING THIS POLICY**

(a) **Corporate Card Payment Systems (Capita Pay360)** - The Council has a corporate Income Management system (AIM) which integrates differing card payment elements. This allows various types of income to be paid using a number of modules as listed below:

- Online (IPay – 3rd party hosted by Capita Pay360)
- Automated Telephone (TouchTone – 3rd party hosted by Capita Pay360)
- Assisted Telephone (Paye.Net – 3rd party hosted by Capita Pay360)

- Kiosk (KPR - imminently will be cash only so will not form part of this Policy)

(b) **Online Processing (IPAY)** - In the first instance, customers should make payment for services online, using the 'Pay Online' link on the Council's website. However only certain payments are set up for payment using this method. This method is one of the two preferred card methods and best practice for taking payments.

On completion of a successful payment, the online payments system will automatically generate an email payment confirmation receipt to the customer.

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 a lack of funds or the card provider suspecting that the transaction could be fraudulent. If a customer faces difficulty in making a payment, they are signposted to Customer Services, where an advisor will be able to answer enquiries and if relevant, take the payment over the telephone using the assisted payment routine (Paye.Net) (see below).

(c) **Automated Telephone (TouchTone)** - The second of the two preferred card payment methods is the fully automated telephone system where the most common payment funds have been added to a secure dedicated telephone payment line. Using 0345 6343001, customers are able to make payment using the telephone keypad to enter their payment and card details.

On completion of a successful payment, a unique customer reference is given to the customer as a receipt number. A series of prompts gives the user the opportunity to note this number as proof of payment or to repeat the receipt number if necessary.

If a customer faces difficulty in making a payment, the telephone system is able to transfer the call to Customer Services (during working hours), where an advisor will be able to answer enquiries and if relevant, take the payment over the telephone using the assisted payment routine (Paye.Net) (see below).

(d) **Assisted Telephone (Paye.Net)** – Payments can be made directly via the service department or with a Customer Services Advisor using the Paye.Net module, where the online or the Automated Telephone Service is not available.

Where card details are provided during the telephone call, these must be processed directly into the Paye.Net screen at the time of contact and must not be written down or noted anywhere.

If it is not possible to submit the card details immediately, then a call back must be requested or offered as soon as available.

Where telephone calls are recorded for training purposes, the telephone recording must stop at the point the staff member using the Paye.Net module enters the payment details screen.

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

Under all three payment options above, there is no internal Council access to full card details as this information is not stored by the Council, either electronic and or in hard copy.

(e) **Storage of Card Details** - Storage of card details on computers in any format (e.g. email, access databases, excel spreadsheets, USB memory sticks) will breach the requirements of the PCI-DSS.

(f) **Data Retention & Disposal** - Information Asset Owners[1] are responsible for complying with the Council's data protection guidelines.

(g) **Electronic Transfer of Data** – The transfer of card data electronically both internally or externally to the Council, is prohibited. This includes the use of end user messaging technologies.

(h) **Refunds** - Refunds can only be processed back to the originating card. The refund must be approved by the responsible Service Manager then forwarded to the person processing the refund. The corporate payments 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 software will not allow the refund to exceed the original amount paid.

9. **REVIEW OF THIS POLICY** - This Policy will be reviewed at least annually, in accordance with the requirements of PCI-DSS, and will be updated when business objectives or the risk environment changes. Queries on this Policy are to be directed to the Customer Services Manager.

[1] See Information Asset Registers for details of Information Asset Owners

Appendix 1

The responsibilities of the following personnel are:

Senior Information Risk Officer

- To manage information security risks highlighted in the Corporate Risk Register.
- To approve high-level information security policies & processes.
- To ensure that an annual audit of PCI - DSS compliance is carried out to ensure continued compliance with the standards, and the review of newly identified risks.
- To ensure that vulnerabilities identified through PCI – DSS compliance testing are addressed as they are discovered.
- To ensure that a risk assessment is carried out upon significant changes to the environment, such as a new payment channel.
- To ensure that any third party company that provides card services on behalf of the Council, is compliant with PCI – DSS.

Data Protection Officer

- To ensure that policies and procedures for protecting cardholder data are documented, in use and known to all affected parties.

Responsibilities of Customer Services Manager (System Administrator)

- To ensure that payment systems never store sensitive information, including the card security code, after a payment has been authorised.
- To ensure that the full PAN is masked on screens, receipts, printouts, etc. The first six and the last four digits are the maximum number of digits that can be displayed.
- To ensure that the maximum amount of information recorded and stored is the card number (rendered unreadable), expiry date and name. This applies to printed receipts, as well as stored electronic information.
- To ensure that access to a payment system is only granted once authorised by the line manager.
- To only grant payment system access to those that require access for the purpose of their role.
- To maintain an audit trail of access authorisation.
- To ensure that the minimum password requirements are set as defined by PCI - DSS requirements.
- Minimum length of at least 7 characters.
- Contains both alphabetic and numeric characters.
- Must be changed at least once every 90 days.
- Must not be the same as any of the last four passwords.
- To immediately revoke the user IDs for any payment system users who no longer requires access.
- To ensure that policies & procedures for identifications and authentication are documented, in use, and known to all parties.

ICT Services

- To ensure that no logs, history or unmasked data are stored.
- To ensure that telephone call recording equipment does not capture & record card details.
- To ensure that cardholder data is encrypted using strong cryptography and security protocols when being transmitted over open, public networks.

- To ensure that policies and procedures for protecting systems against malware are documented and in use and known to all affected parties.
- To ensure that anti-virus software is installed on all systems at risk of being affected by malicious software. The software must be capable of detecting, removing and protecting against all known types of malicious software.
- To ensure that anti-virus software in use is kept current and actively running, performs periodic scans and generates audit logs.
- To ensure that anti-virus software cannot be disabled or altered by users, unless specifically authorised by management for a limited period.
- To inform the SIRO and DPO once a vulnerability has been identified, detailing the risk identified and to discuss plans for remediation.
- To assist in the annual audit of PCI- DSS compliance, providing information on how the networks and system meet up-to-date PCI – DSS requirements.

Senior Managers

- To ensure that appropriate controls are in place for physical areas where cardholder data is processed, to prevent accessibility of cardholder data by unauthorised persons.
- To immediately notify the Customer Services Manager when a [staff] user within their remit no longer requires system access.
- To ensure that all staff are aware of this Policy.

All Staff

- To ensure that cardholder data, including the card security code, is never written down and it is never stored unencrypted after a payment has been authorised.
- To ensure that card numbers are **never**, sent in emails, instant messaging, chat or any other end-user messaging. This includes card numbers captured as part of a screen dump.
- To ensure that no cardholder data should ever be taken or stored off council premises.
- To ensure that card numbers and security codes are not repeated in full back to customers in an area that can be heard by others.
- To ensure that cardholder data is never copied, moved or stored onto local hard drives or removable media, such as memory sticks.
- To ensure that personal login details are kept safe and never shared with others, and passwords are changed if there has been a risk of passwords being shared or known by others.

Version Control

Version	Description of version	Date
1.0	Security Policy – Processing Electronic Card Payments	November 2019