BRIDGWATER GUY FAWKES CARNIVAL – CARD TRANSACTION POLICY

1. 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 organisations card provider. Organisations that fail to meet the compliance requirements risk losing their ability to process card payments and being audited and/or fined.

To reduce the Committee's exposure to compliance costs and the risk of non-compliance, the Committee seeks to eliminate all processing of credit card data – transferring that responsibility and the requirement to be PCI DSS compliant to an accredited third party processor, in the case of the Carnival Committee PayPal. By doing so the Committee will be taking steps to minimise the aspects of the PCI DSS standard to which it has to adhere. Any member who comes into contact with cardholder data needs to be aware of PCI DSS, and how they as an individual can reduce the risk of cardholder data theft and fraud.

2. Purpose of this 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 control of the Committee that come into contact with cardholder data, whether these be electronic or paper based.

3. PCI-DSS Applicability to the Committee

The Committee is a 'Level 4 Merchant which means that certification to the Standard requires the completion of an annual self-assessment questionnaire (SAQ C-VT) to demonstrate compliance.

4. Definition of Cardholder Data

Cardholder data consists of 2 main sets of data that must be protected by the Committee 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

5. PCI DSS requirements

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.

r

6. Responsibility and Internal Control

The management and control of information received, in respect of cards applies to all members 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:

- Access to payment card transactions and data must be restricted to only those members who need access as part of their role.
- Members (where required) 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 methods.
- All details of payments and card details should be kept secure and never left on public view.
- Merchant copies of payment receipts and card details must be retained in a secure, locked cabinet or room at all times and cross shredded immediately after use.
- Customer's card details should never be sent by email.
- If taking an order by phone you should not repeat the card information in the hearing distance of others, if you wish to check ask the customer to repeat the information.

7. Committee Approved Card Payment Methods and Services

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

COMMITTEE APPROVED PAYMENT METHODS				
Payment Method	**Approved Payment Services**	**Card Transaction**	**Mandatory Controls**	**Storage of Card Data**
Customer Not Present	**Online**	**Web Application Transaction**	Payment via an online system should generate an email payment confirmation to the customer. This should be the only confirmation document received by the customer from the Committee for the transaction.	**Data is held by the Committee PCI-DSS compliant approved suppliers PayPal or Stripe**
			If a customer's payment has been unsuccessful or declined, the customer should contact their card provider in the first instance.	
			If a customer faces difficulty in making a payment then staff assistance can be provided.	
			If the payment problem cannot be resolved, the customer should provide a number to be called back on at a suitable time or offered an alternative payment method.	

Payment Method	Approved Payment Services	Card Transaction	Mandatory Controls	Storage of Card Data
Customer Present	**Centre**	**Virtual Terminal**	If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the customer.	**ONLY merchant receipts should be held in physical secure storage, no card details.**
			If the transaction is declined, the customer should be advised immediately and given the option of paying with a different card.	
Customer NOT Present	**Telephone or Post**	**Virtual Terminal**	Where card details are provided during a telephone call or by post, these must be processed directly into the online payment system at that time. The card details must not be written down and kept.	**Card details must not be left lying around or stored, once used shred!**
			When card details are being provided during a telephone call these must not be repeated back to the customer in such a way that it can be intercepted by third parties.	
			If it is not possible to submit the card details immediately then a call back must be offered.	

8. 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)
- **Pin or CVC type numbers should never be stored**.

9. Approved Payment PCs and area(s)

The Committee has taken all appropriate steps to ensure any risks to members and payment services have been reduced and mitigated accordingly, to allow secure payments to be undertaken in line with regulative controls.

10. Refunds

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

r

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.

11. 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.

12. Secure Disposal

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

13. Third Party Approved Suppliers

Any third party appointed to manage card holder data on behalf of the Committee must be an approved and trusted partner. The third party must be audited on an annual basis and PCI-DSS certification must be evidenced.

14. Requirement

Maintain a policy that addresses information security for all personnel.

Notes:

PayPal allows buyers to dispute transactions for 180 days, so hold onto your records after a transaction is complete. PayPal offers a seller protection policy for physical items that are shipped to buyers. To qualify, you must ship to the address on the transaction details page, and respond quickly to requests for documentation. "That covers sellers if buyers claim they didn't receive an item, and the seller can prove it was shipped. Seller protection also protects sellers from fraudulent or unauthorised payments."

- The Payment Card Industry Data Security Standard (PCI DSS) was developed by the major card brands to protect credit card information.
- The PCI DSS is mandatory for all entities that store, process or transmit cardholder data, including merchants and service providers.
- PCI DSS compliance is usually enforced by a merchant's acquiring bank.
- There are four different merchant levels depending on the number of payment card transactions processed each year. The merchant level directly impacts compliance validation requirements.
- PCI DSS compliance must be maintained continuously to help protect against costly cardholder data compromises, for which all card-accepting businesses are at risk.
- According to Trustwave SpiderLabs' Global Security Report 2012, 89% of data targeted by hackers in 2011 was customer records - including cardholder data and other PII. PCI DSS compliance helps to keep this information secure.