Bodmin Town Council
Information Security Policy

Document Name & Version:
Information Security Policy - BTC – 17.11.22 - VFA 4.0

Responsible Officer: Senior Accounts Officer

Date approved by Full Council Committee: 17th November 2022

Date adopted by Council: 17th November 2022

Review Date: 17th November 2023

1 Introduction

1.1 This document aims to protect the confidentiality of data and ensure adequate security measures are in place. It reflects Bodmin Town Council's commitment to comply with the required standards governing the security of sensitive and confidential information, specifically with regards to the Payment Card Industry Data Security Standard (PCI-DSS).

It establishes the rules to insure the protection of confidential and/or sensitive information technology resources and data, against acts such as misuse and/or loss. It details the responsibilities and authority of information users.

1.2 For the purposes of this document, '*information security*' is defined as the preservation of confidentiality which includes:

- Protecting information from unauthorised access and disclosure
- Safeguarding the integrity, accuracy and completeness of all information and associated processes

Information exists in many forms. It may be printed, handwritten or stored electronically. It can be transmitted by post, using electronic means or spoken. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

2 Information Security Responsibilities

2.1 Bodmin Town Council will ensure that:

- Someone is specifically responsibility for Information Security in the organisation - currently the Senior Accounts Officer (SAO) is nominated as the Chief Security Officer (ChSO), who must ensure that the policy complies with all standards such as the PCI-DSS.

- That information security is the responsibility of all members of staff who use information technology resources.

2.2 The Chief Security Officer will ensure that:

- The information security policy and updates are distributed to all relevant staff.

- Every person handling information or using information systems is aware and must adhere to the Information Security Policy and procedures during and where appropriate after the termination of their employment with Bodmin Town Council.

- Security incident response procedures are issued to all relevant members of staff.

2.3 The Community Services Officer (Town Council Reception) and the Chairman of the Museum (Museum Shop) will:

- monitor access to sensitive cardholder data.

2.4 For a breakdown of responsibilities see the table in Annex 1b

3 Protect Sensitive Data

3.1 Sensitive and/or confidential data must be protected when stored at all times, especially when in transit from one secure location to the next secure location.

Bodmin Town Council does not store any electronic sensitive card holder data.

4 Storage of Card/Cardholder Data

4.1 Records of sensitive credit card authentication data must never be stored or recorded, data such as:

- Any form of magnetic strip data from the card (Track)
- Card Validation Codes (CVC) or,
- Personal Identification Number (PIN)

4.2 Sensitive data must never be transmitted over public networks or via end-user messaging technology (e.g. wireless networks, e-mail, instant messaging etc).

4.3 The credit card Primary Account Numbers (PAN) must be masked or truncated on all media, except for those users who have a valid business need to see full PAN data in line with PCI-DSS.

Bodmin Town Council does not provide this information to any users.

***5* Restrict Access to Sensitive Data**

5.1 The Council restricts access to cardholder data and systems on a business need to know basis. Currently the following members of staff have access to this information

- Community Services trained card processing staff.
- Accounts team for the purposes of handling receipts.
- Museum trained card processing volunteers.

5.2 Only trained Community Services staff and Museum Volunteers have authority to take cardholder data by processing card payments on a chip and pin terminal (Community services) or a Card reader device (Museum). Authority is given when considering Role Based Access Control (RBAC).

For more information about the members of staff and the level of authority

please see Annex 1a.

6 Securing Hardcopy Materials

6.1 Bodmin Town Council will ensure that all hard copy materials containing cardholder data are protected and kept secure at all times.

For detailed information on the card processing procedures/rules which include the control of internal distribution, labelling and storage, please see Annex 2.

6.2 All relevant Community Services/Accounts staff and Museum Volunteers must be trained to ensure they are fully conversant with these procedures, which must be followed at all times.

All staff/Volunteers working with sensitive card holder data must sign the Agreement to comply with the Information Security Policy. For an example of this agreement please see Annex 3.

7 Media Destruction

7.1 All media containing cardholder data is destroyed when it is no longer needed for business or legal reasons, currently the time period for retaining this information is in line with the HMRC VAT guidelines.

For detailed information on the procedures/rules for destruction please see Annex 2.

8 Employee Facing Technologies

8.1 Bodmin Town Council does not currently use employee-facing technologies for providing or using sensitive cardholder data. However, for all other information technology resources employees must only use the technology which they are authorised to use. A list of these devices is maintained by the Accounts Department.

The Council has a separate email and internet usage policy.

The Council has a Document Retention policy.

9 Sharing Data with Service Providers

9.1 Bodmin Town Council will not normally share any sensitive card holder information with third parties or service providers.

However, should there be a business requirement to do so, then this would only be done following a formal written agreement between Bodmin Town Council and the Service Provider, acknowledging the responsibility for securing all cardholder data as required by PCI-DSS, and the service provider would need to be PCI DSS compliant.

10 Review and Amendment of Policy

10.1 The Information security policy will be reviewed annually or earlier if required to reflect changes in the risk environment (such as new protection measures to fight against threats, as security threats and protection methods evolve rapidly) or due to changes in the industry.

It will be prepared by the Senior Accounts Officer for approval by the Policy & Resources Committee.

The Council reserves the right to make variations to this policy at any time, subject to approval of full Council. Any variations will be made available to the public.

11 Alternative Formats & Other Queries

11.1 If you need this information in a different format or have any other queries regarding this policy, please contact us:

- by email: info@bodmin.gov.uk
- by phone: 01208 76616
- by post: Shire Hall, Mount Folly, Bodmin, PL30 2DQ

ANNEX 1

a) Assignment of Employee Roles and Responsibilities for Security

Name of Individual or Group	**Date Assigned**	**Description of Responsibility**	**Type**
CS Assistants, Senior Information Officer, CSO & CSM/ATC Museum Volunteers		Process card payments, including 'card not present'	Chip and Pin Device
Accounts Assistants		Recording and security of hard copy card receipts.	Hard Copy Receipts
SAO/TC		Authorisation of Movement of card holder data, control of inventory records and destruction of data.	Hard Copy Receipts
/CSO/SAO/ Chairman of Museum		Authorisation of Movement of card holder data.	Hard Copy

b) Assignment of Management Roles and Responsibilities for Security

Name of Individual or Group	**Date Assigned**	**Description of Responsibility**
SAO		Establish, document and distribute security Policy
SAO		Monitor, analyze and distribute security alerts and information
SAO		Establish, document and distribute security incident response and escalation procedures
CSO & Chairman of Museum		Monitor and Control all access to cardholder data, using RBAC.

ANNEX 2

All relevant staff must act in accordance with the following procedures/rules at all times;

BODMIN TOWN COUNCIL CARD PROCESSING PROCEDURES

Only authorised staff/ volunteers may use the card processing device, please see Annex 1a for individual responsibilities.

General

- The Reception accepts credit and debit cards for payment for goods and services. Accepted cards are Visa, Maestro, Diner Club and Mastercard. The Bodmin Information Centre does not currently accept American Express for payment.

- The Museum accepts credit and debit cards for payment for goods. Accepted cards are Visa, Mastercard, American Express, Discover. The device also accepts NFC forms of payments such as Google Pay and Apple Pay.

Bodmin Town Council Reception

Face to Face Customer Transactions Procedure

1. Enter all purchases in the till prior to taking payment.

2. Advise the customer of the total price due and take the card from the customer.

Either

A) Chip & Pin

3. Ask customer to place the card (chip face up) into the front of the handheld. Follow the on-screen instructions to input payment and press enter.

4. Double check the correct amount payable is entered into the machine.

5. When prompted for the customer's pin, give the handheld machine to the customer; and ask them to check the amount, if correct then enter their pin number and then press the green button

6. **IF THE CUSTOMER DOES NOT KNOW THEIR PIN ASK FOR AN ALTERNATIVE PAYMENT METHOD/CARD**

7. Once the customer has entered a correct pin number, replace the PDQ machine back onto the battery pack and wait for the transaction to be authorised.

B) Contactless

8. Follow on screen instructions to input payment amount then press enter.

9. Double check the correct amount payable is entered into the machine.

10. Ask Customer to tap card against the screen of the PDQ.

For all methods of card payments

11. If the transaction is declined, repeat/ carry out steps 4 to 8. If the card is declined a second time, ask the customer for alternative method of payment.

12. The PDQ will automatically print the merchant copy receipt whether the payment has been authorised/ declined

13. Follow the on screen instructions (Press F1) to print the customer a copy of the receipt if required.

    The first receipt the 'merchant copy 'MUST be retained by Bodmin Town Council. The receipt needs to be checked to ensure that either the pin has been verified. 'PIN VERIFIED' or for contactless payments 'No Cardholder verification' and an Authorisation Code I shows on the receipt and must be highlighted by the staff member. This is essential as the PDQ machine does not highlight if the transaction has been declined, it will just state 'DECLINED' on the receipt. The merchant copy needs to be stored securely in the till immediately.

    The second receipt states 'customer copy' and should be passed to the customer (double check to ensure the correct copy of the receipt is being passed to the customer) with till receipt and items sold. If the customer does not require the customer copy this needs to be shredded immediately.

PLEASE NOTE NO ITEMS SOLD INCLUDING TICKETS SHOULD BE PASSED TO THE CUSTOMER UNTIL PAYMENT HAS BEEN COMPLETED AND VERIFIED.

Occasionally HSBC will run a random card check. When this happens a message will appear on the PDQ machine with a contact number. Call the number and follow the instructions from the HSBC advisor. The check will either result in authorisation of the payment. However if the payment is then declined, it may be that the card is stolen or the use is fraudulent, the HSBC advisor will explain the appropriate course of action.

International Cards without CHIP and PIN - Face to Face Customer Transactions Procedure

Some international credit and debit cards do not have a chip and pin element and therefore require a signature.

1. Enter all purchases in the till prior to taking payment.

2. Advise the customer of the total price due and take the card from the customer.

3. Double check the correct amount payable is entered into the machine.

4. Swipe the card on the side of the PDQ and follow the on screen instructions.

5. The PDQ will then produce a receipt requesting a customer signature. Tear off the receipt and ask the customer to check the amount and then provide their signature in the appropriate place. The assistant should retain the customer's card.

6. Take the signed receipt and check the signature against the reverse of the card. If they match, follow the on-screen instructions to confirm the match. A second customer receipt will print out which you should give to the customer along with their goods. The signed receipt should be retained by the assistant, attached to the till receipt and put in the cash register drawer.

7. **IF THE CUSTOMER'S SIGNATURE IS NOT VISIBLE ON THE CARD OR DOES NOT MATCH, ASK FOR AN ALTERNATIVE PAYMENT METHOD/CARD.**

8. If the transaction is declined, repeat steps 4 to 8. If the card is declined a second time, ask the customer for alternative method of payment.

Telephone Customer Transactions Procedure

Customers may wish to pay for goods or services over the telephone such as;, National Express tickets or room hire bookings/deposits.

PERSONAL DETAILS INCLUDING CREDIT CARD NUMBERS AND PINS MUST NEVER BE WRITTEN DOWN OR RECORDED.

IF THE PDQ MACHINE IS NOT FREE AT THE POINT YOU WISH TO PROCESS PAYMENT PLEASE TAKE THE CUSTOMERS CONTACT DETAILS AND CONTACT LATER.

1. Inform the customer of the total value of the services including postage (if applicable) and then ask for the card details. Check that the customer card type is accepted by HSBC (as listed under the general section).

2. Inform the customer that you will require the following information to process the transaction. The name on the card holder; the long 16 digit card number, the card start and expiry date; the three digit security code on the reverse of the card and the full address and postal code that the card is registered to.

3. Whilst on the telephone to the customer use the keyed and customer not present method enter the card details into the hand held machine and follow the onscreen instructions, requesting the information as prompted for it by the PDQ machine.

4. At the point of authorisation, the machine will inform you of the level of matches that the card has achieved.

   For example,

   a) Security code only match.

      - Proceed if the total payment is below £ **In 2022/23 this is £20.00**.
      - Proceed if the payment is for an invoice that has been raised for services already received i.e. Shire Complex room hire

   b) If a full match is obtained and the payment is authorised, print the two receipts

      The first receipt will be the 'merchant copy' and is to be retained by Bodmin Town Council. This must be checked to ensure that the payment has been authorised. 'An authorisation code will show on the receipt and must be highlighted by the staff member. This is essential as the PDQ machine does not highlight if the transaction has been declined, it will just state 'DECLINED'.

      The second receipt states 'customer copy' and should be forwarded to the customer for their records.

5. If the transaction is declined, repeat steps 3 to 4. If the card is declined a second time, or a full match is not obtained ask the customer for alternative method of payment.

Museum Shop

Face to Face Customer Transactions Procedure

1. Enter all purchases in the till prior to taking payment.
2. Advise the customer of the total price due.
3. Enter the transaction amount and press the green tick. Double check the correct amount payable is entered into the machine.
4. "Press tap" will appear on the screen then the customer can either A) Contactless payments - tap their contactless-enabled card or device against the screen of your card reader. The reader will beep and the four LED lights will flash to confirm a successful payment.

   Or
   B) give the handheld machine to the customer; and ask them to insert their card and enter their pin number and then press the green tick to confirm.

5. **IF THE CUSTOMER DOES NOT KNOW THEIR PIN ASK FOR AN ALTERNATIVE PAYMENT METHOD/CARD**

6. If the transaction is declined, repeat steps 4 to 7. If the card is declined a second time, ask the customer for alternative method of payment.

7. Once the payment has been authorised you will see the notification "send receipt" you can choose to send a receipt via

   - Email receipt – enter customer details and press green tick.
   - SMS receipt – enter customer details and press green tick.
   - Print receipt (if printer is attached) – Select Print receipt.

8. Card receipts are not to printed and stored by the Museum.

BODMIN TOWN COUNCIL DOES NOT PERMIT MEMBERS OF STAFF/ VOLUNTEERS TO RELAY PERSONAL INFORMATION SUCH AS CARD INFORMATION TO A THIRD PARTY, EVEN WITH VERBAL CONSENT.

BODMIN TOWN COUNCIL CARD PROCESSING RULES

Bodmin Town Council will adhere to the following rules in regards to;

Storage, Transmission and Transferring Data

- Employees or Volunteers must: Never store any sensitive or confidential card holder data on any information technology resource which includes;
    - Information from the magnetic strip data on the card (Track)
    - Card Validation Codes (CVC)
    - Personal Identification Number (PIN)
- Ensure that the Primary Account Number (PAN) is masked or truncated on all media except for the Merchants copy.
- Never transmit card holder data via end-user messaging technologies
- Ensure that all media is physically secured at all times
- Ensure that all card holder information is classified as sensitive information and is labelled as confidential.
- Ensure that all receipts only be hand delivered to and by authorised members of staff to ensure secured protection at all times
- Must never share data with third parties or service providers

Media (Hard Copy Receipts) Destruction

When media containing card holder information is destroyed it must be done following these rules;

- Permission must be obtained from the Chief Security Officer
- The inventory must be updated when information has been destroyed

- Information will not be kept longer than needed for business or legal reasons – currently this is in line with the HMRC VAT guidelines (six historic years plus current year)
- All hard copy materials must be destroyed with a cross-shredder
- All hard copy materials must be kept secure prior to being destroyed, after being removed from the secure location.

Management of Information

- All staff/ volunteers must report any incidents of non-compliance to the Town Clerk/ Senior Accounts Officer
- An inventory of data must be kept, which details the receipt numbers, location and date destroyed
- Policy updates will be provided to each authorised member of staff after approval of the Council by the ChSO

ANNEX 3

Agreement to Comply with the Bodmin Town Council Information Security Policy

(All employees/ Volunteers working with sensitive cardholder data must submit a signed paper copy of this form to the Senior Accounts Officer)

Employee/ Volunteer Name:

Department:
(Including address)

I, the user, agree to take all reasonable precautions to ensure that Bodmin Town Council's internal information, or information that has been entrusted to Bodmin Town Council by third parties such as customers, will not be disclosed to unauthorised persons.

I agree to return to Bodmin Town Council all information to which I have had access as a result of my position within the Council. I understand that I am not authorised to use this information for my own purposes, nor am I authorised to provide this information to a third party without written consent from the Senior Accounts Officer who is the designated Chief Security Officer.

I have access to a copy of the Bodmin Town Councils Information Security Policy and I have read and understood how it impacts my job. As a condition of my continued employment/ volunteering with Bodmin Town Council I agree to abide by this policy and its procedures. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I agree to promptly report all violations or suspected violations of information security to the Town Clerk.

Employee/ Volunteer Signature:

Date:

ANNEX 4
Glossary

Payment Card Industry Data Security Standard – PCI-DSS
Senior Accounts Officer - SAO
– Community Services Officer - CSO
Chief Security Officer – ChSO
CSM/ATC – Community Services Manager/ Assistant Town Clerk
Card Validation Code – CVC
Personal Identification number – PIN
Primary Account Number – PAN
Role Based Access Control – RBAC
Finance, Staffing and Performance Management - FSPM