Town Council Information Security Policy for the Use of Chip and PIN
Reviewed by the RGS Committee at its meeting on 8 April 2026

1. Purpose

This policy sets out the information security requirements for the use of Chip and PIN payment devices by the Town Council. Its aim is to ensure that all cardholder data is protected, that the Council complies with relevant legal and regulatory obligations, and that risks associated with payment processing are minimised.

2. Scope

This policy applies to:

- All Chip and PIN terminals owned, leased, or used by the Town Council
- All staff, councillors, and volunteers who handle card payments
- All locations where card payments are taken (e.g., reception, events, ticket offices)

This policy covers the processing of card payments but **does not** permit the storage of cardholder data in any form.

3. Principles

The Town Council will ensure that:

- Cardholder data is handled securely and confidentially
- Only authorised personnel operate Chip and PIN devices
- No cardholder data is stored electronically or in paper form
- All devices are protected against tampering, loss, or misuse
- The Council complies with PCI DSS requirements applicable to its operations

4. Roles and Responsibilities

Town Clerk

- Ensures compliance with this policy
- Maintains a register of all Chip and PIN devices

- Ensures staff receive appropriate training
- Ensure staff handbook is issued for all new joiners detailing the process for chip and pin
- Ensure copy of this policy is given to all new joiners.

Staff and Volunteers

- Must follow this policy and all associated procedures
- Must report any suspected security incident immediately
- Must not attempt to repair, alter, or modify devices

Finance Officer

- Oversees reconciliation of Chip and PIN transactions
- Ensures secure handling of receipts and financial records

5. Device Security

- All Chip and PIN devices must be kept in a secure location when not in use.
- Devices must be inspected daily for signs of tampering (e.g., loose parts, unfamiliar attachments).
- Any suspicious activity or device irregularity must be reported immediately to the Town Clerk.
- Devices must only be connected to approved networks or mobile data connections.
- Devices must not be left unattended during a transaction.

6. Handling Cardholder Data

The Council will comply with PCI DSS by ensuring:

- **No cardholder data is stored** on Council systems, paper forms, or personal devices.
- Staff must never write down card numbers, expiry dates, or security codes.
- Receipts must not display full card numbers or sensitive authentication data.
- Cardholder data must not be transmitted via email, messaging apps, or unencrypted channels.

7. Transaction Processing

- All transactions must be processed through the approved Chip and PIN terminal.
- Staff must verify that the amount entered is correct before the customer inserts or taps their card.
- Staff must not handle a customer's PIN or attempt to observe it.

- If a transaction fails, staff must follow the approved troubleshooting procedure and must not request card details verbally.

8. Training

All staff and volunteers who process payments must receive training covering:

- Secure use of Chip and PIN devices
- Recognising signs of device tampering
- Handling cardholder data securely
- Incident reporting procedures

Training must be refreshed at least every two years or when significant changes occur.

9. Incident Reporting

Any of the following must be reported immediately to the Town Clerk:

- Suspected or actual loss of cardholder data
- Device tampering or theft
- Suspicious behaviour by customers or staff
- System failures affecting payment processing

An incident log will be maintained, and serious incidents may be reported to the acquiring bank, PCI authorities, or the ICO where required.

10. Physical Security

- Devices must be stored in locked cabinets or secure rooms when not in use.
- Access to devices is restricted to authorised personnel.
- Devices used at events must be transported securely and signed in/out.

11. Auditing and Compliance

- The Town Clerk will conduct an annual review of compliance with this policy.
- The Finance Officer will reconcile transactions regularly to detect anomalies.
- The Council will complete any required PCI DSS self-assessment questionnaires (SAQs).

12. Policy Review

This policy will be reviewed every two years or sooner if:

- PCI DSS requirements change
- New payment technologies are introduced
- A security incident indicates a need for revision