



STANDING OPERATING PROCEDURE

Subject	Payment Card Industry Data Security Standard (PCI DSS) SOP044
Applicable to	All staff and volunteers who have access to POI (Point of Interaction) devices across Nottinghamshire Hospice.
Date issued	July 2024
Next review date	July 2025
Lead responsible for Policy	Director of Income Generation
Policy reviewed by	Director of Income Generation
Policy written by	Retail Operations Manager
Notified to	Policy Working Group 11 June 2024
Authorised by	Senior Leadership Team (July 2024)
Links to other Policies/Procedures	Information Security and Data Protection Policy
Summary	This procedure aims to clarify how Nottinghamshire Hospice will comply with PCI DSS standards and requirements.
Target Audience	All staff and volunteers across Nottinghamshire Hospice where Point of Interaction (POI) devices are used to take payment from customers and donors.

IMPORTANT NOTICE

Staff should refer to the Hospice website for the most up to date Policy. If the review date has passed it is still valid for 3 months. After that staff should seek advice from their clinical lead or manager.

<p>1.</p>	<p>Introduction</p> <p>This procedure is to ensure that all parties involved in taking card payments from customers and donors are fully aware of the procedures to ensure that Nottinghamshire Hospice comply with Payment Card Industry Data Security Standards (PCI DSS).</p> <p>Nottinghamshire Hospice uses Point of Interaction (POI) devices (also known as card terminals) supplied by Elavon.</p>
<p>2.</p>	<p>Security of POI Devices</p> <p>Nottinghamshire Hospice are required to meet security standards to ensure that POI devices are not tampered as this could result in compromised customer data.</p> <p>Nottinghamshire Hospice will follow the following steps:</p> <ul style="list-style-type: none">• POI integrated chip and pin devices were installed by an engineer in all Nottinghamshire Hospice stores. No changes will be made to the device set up.• The Fundraising team have access to a mobile POI device which is located in the Fundraising office. The POI device is protected by a PIN when not in use and the Fundraising office is locked overnight.• If the mobile POI device is taken to offsite events every effort will be made by the member of the staff in charge to ensure its safety. If the mobile POI device is misplaced or stolen, this will immediately be reported via normal channels and escalated to the Director of Income Generation.• Manuals are held and available to refer to as required.• POI device surfaces will be examined on a quarterly basis to detect tampering and unauthorised substitution. The Retail Operations Manager will prompt these checks and record the outcome.• Identification will be requested, before any third party is granted access to modify or troubleshoot devices.• If in any doubt advice should be sought from the Retail Operations Manager.

3. Training

All staff and volunteers involved in taking customer/donor card payments should read and action the following steps:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Advice should be sought from Retail Operations Manager before the third party is given access to the POI device.
- No POI devices should be installed, replaced, or sent anywhere without consulting the Retail Operations Manager.
- Follow Retail Operations Manager instructions if devices need installing, replacing, or returning.
- Being aware of suspicious behaviour around devices and immediately report to your line manager who will escalate to Retail Operations Manager.
- Report suspicious behaviour and indications of device tampering or substitution to your line manager who will escalate to Retail Operations Manager.

4. Use of POI Devices

All POI devices should be used in line with the manufacturer instructions.

To ensure the safety of cardholder data all staff and volunteers involved in taking customer/donor card payments should read and action the following steps:

- Never write down or record in any other way, a card number, expiry date or CVV code (3-digit code on the signature strip on back of the card).
- Always avert eyes when a customer/donor is entering their PIN.
- If a customer/donor leaves their card in error, this should be immediately locked in the safe and the Retail Operations Manager informed.

5. Emergency Contact

The Retail Operations Manager should be contacted in the event of an emergency relating to POI devices.

Telephone Number: 07812 510893

Email: paula.watkins@nottshospice.org