

Payment Card Security Policy

Northgate Primary School



Approved by: Northgate Governing Body

Last reviewed on: March 2023

Next review due by:

Background

Northgate Primary School accepts debit and credit card payments online and in person (face-to-face). In person payments are processed on a physical payment device. The payment device is stored in the main school office and charged each night.

The Payment Card Industry Data Security Standard (PCI-DSS) is a mandatory standard that all organisations accepting card payments must adhere to. The purpose of the standard is to reduce the risk of theft and fraud of sensitive cardholder data by providing a secure environment for customers to make payment. In the event of a data breach, failure to comply with the standard will result in higher fines and increased transaction charges and may result in removal of permission to accept card payments, and further investigation by other regulatory bodies such as OSCR and the ICO.

Northgate Primary School must demonstrate its compliance with the standard by completing an annual self-assessment questionnaire (SAQ), or more frequently if there is any change to the payment card environment, for example introducing new methods of card payment or changing devices.

This policy assists Northgate Primary School in complying with the legal requirements of the Payment Card Industry Data Security Standard. It will assist in reducing the risk and impact of a data breach, including subsequent fines and charges, and it ensures adequate safeguards are in place to protect sensitive cardholder data. Failure to comply with this policy may result in disciplinary action.

Responsibilities

Both a member of staff and JSPC Computer Services, our external IT contractors, undertakes the requirements of PCI-DSS compliance.

JSPC are responsible for providing a secure internal network environment that adheres to all payment card security standards not limited to but including secure internet.

The Head Teacher of Northgate Primary School is responsible for ensuring the school is compliant with PCI-DSS.

Schools with card payment devices (physical or virtual) are responsible for adhering to all policies relating to payment card acceptance including nominating a point of contact for queries or issues and ensuring all staff with access to cardholder data or devices undertake the mandatory annual payment security training.

Accepting Card Payments

New or changes to existing card payment methods (virtual or physical) must be requested through and approved by Head teacher or Business Manager.

Miss Watson will maintain a register of all card payment methods and devices.

The need for payment card devices should be reduced by processing sales through the online payment system, SCOPAY. However, it is recognised in some instances there may be a genuine need to accept card payments as ease for parents and carers.

All Schools accepting payment by card (in any format) must adhere to all policies and procedures detailed in this and other supporting documentation, failure to do so may result in the removal of the payment device and the area being unable to accept card payments.

Payment methods that are implemented without obtaining the appropriate permissions and/or do not meet the required standards will be removed from service.

Payment Card Devices

All payment card devices (virtual or physical) must be requested through and approved by the Head Teacher or Business Manager.

Miss Watson will maintain a register of all such devices including location, unique device identification numbers, model type and key contacts.

All payment card devices must have end to end encryption. End to end encryption means the payment data is transmitted to the payment service provider in an encrypted (unreadable) format. The payment service provider holds the decryption code to decipher the transmission and process the payment.

To reduce the risk of a data breach, payment card devices capable of storing or transmitting unencrypted data must not be used or connected to any system or network including WIFI.

Payment card devices must not be added to the school's network without prior consultation and authorisation from the Head Teacher or Business Manager. This includes devices using WIFI, blue tooth, GPRS, or any other transmission method.

Payment Card Device Security

Our physical card device will be located in a secure environment. It will not leave the office or be taken away to make payments off-site.

If the device is left unattended it must be appropriately secured or removed to a secured location e.g. in a locked office.

All devices must be inspected regularly, and as a minimum before the commencement of service. The purpose of inspecting devices is to identify signs of tampering at the earliest opportunity and so reduce the impact of fraud. Tampering may be in a physical form such as skimming devices or swapping of terminals, or a change in performance which may indicate the presence of malware.

Schools are responsible for undertaking regular device inspections in accordance with the Card Payment Device Inspection Procedure. We will request this will be done by JSPC Computer Services.

Payment Card Receipts

The default setting for the payment machine is the first payment card receipt contains sensitive cardholder data i.e. the full card number or PAN (primary authentication number). All first receipts are given back to the parent or carer as their copy and proof of payment. The second copy of the receipt is printed which does not contain the PAN.

All receipts, regardless of whether the PAN is displayed in full or not, must be treated as sensitive data and be stored in a secure location or shredded if not needed to be kept and disposed of in sensitive waste.

Receipts on which the PAN is obscured must be disposed of no later than one month after the date of sale.

Receipts on which the full PAN is displayed must be disposed of securely in a sealed confidential waste bag. The confidential waste bag must be stored securely in a restricted location until collection.

Cardholder data must not be used for any other purpose than that intended i.e. payment acceptance and related refunds.

Staff Training

All staff are responsible for adhering to Northgate Primary School policies regarding payment acceptance and security.

Staff with access to the cardholder data must undertake mandatory annual Payment Acceptance training. This includes:

- All staff who accept card payments, even if infrequently

Training will include, but is not limited to, understanding the importance of payment card data security, device security, and the incident response plan.

Incident Response

Miss Watson will work with JSPC to maintain the Incident Response plan.

In the event that an incident is identified e.g. a payment device is suspected of being tampered with, the School must remove the device from service immediately and unplug it from networks and/or systems.

The nominated individual identified on the Payment Card Device Inspection Procedure should be contacted immediately (JSPC).

The nominated individual will investigate the matter, if satisfied the device has not been tampered with it can be returned to service.

If there is any concern over the security or integrity of the device, it must not be returned to service.

All incidents must be logged and reported to Miss Watson who will undertake further investigations if required.

If the nominated individual and their delegated substitute are both absent the device must be removed from service and the incident reported to the Business Manager immediately.

Data Protection Officer is responsible for reporting data breaches to the appropriate third parties.

The Incident Response Plan will be reviewed annually.