NCG Cardholder Information Security Policy

Policy Title	NCG Cardholder Information Security Policy
Policy Category	Compliant
Owner	Financial Transactions Manager
Group Executive Lead	Chief Finance Officer
Date Written	February 2021
Considered By	Executive Board
Approved By	Executive Board
Date Approved	March 2021
Equality Impact Assessment	The implementation of this policy is not considered to have a negative impact on protected characteristics
Freedom of Information	This document will be publically available through the Groups Publication Scheme.
Review Date	March 2024
Policy Summary	NCG Cardholder Information Security Policy - This policy serves to provide guidance on the handling of sensitive cardholder data in order to protect cardholder and account privacy and to ensure compliance with the Payment Card Industry legislation (PCI DSS v3.2.1). This policy applies to all NCG staff handling cardholder information.

Applicability of Policy	Consultation Undertaken	Applicable To
Newcastle	No	Yes
Newcastle 6th Form	No	Yes
Carlisle	No	Yes
Kidderminster	No	Yes
Lewisham	No	Yes
Southwark	No	Yes
West Lancashire	No	Yes
Professional Services	No	Yes

Changes to Earlier Versions	
Previous Approval Date	**Below are main changes made in this version**
n/a	NCG Cardholder Information Security Policy not previously considered/approved by Executive Board
Linked Documents	
Document Title	**Relevance**
NCG Card Payment Procedure	NCG Card Payment Procedure describes the processes to support the policy.
NCG – Standard Operating Procedure – PCI-DSS Governance	NCG – Standard Operating Procedure – PCI-DSS Governance provides the NCG PCI-DSS compliance commitments behind the policy and describes the internal review process carried out to ensure continued compliance with PCI-DSS.

1. Purpose of this Policy

1.1. This policy serves to provide guidance on the handling of sensitive cardholder data in order to protect cardholder and account privacy and to ensure compliance with the Payment Card Industry legislation (PCI DSS v3.2.1).

1.2. This policy applies to all NCG staff handling cardholder information. All staff must read this document in its entirety and sign the form confirming they have read and fully understand this policy.

1.3. The policy shall be reviewed every 3 years and updated if regulations change in the interim.

2. Background

2.1. NCG staff handle customer and account information daily. This data is sensitive and confidential. All organisations handling card payment data (processing card payments) are required to comply with the Payment Card Industry (PCI) Data Security Standard v3.2.1.

2.2. The Payment Card Industry (PCI) Data Security Standard v3.2.1 was adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of a number of steps and security best practices that help to ensure the secure processing of sensitive data.

2.3. Sensitive Account (cardholder and sensitive authentication) Data must be protected at all times. This account data consists of two main sets of data as shown in below table.

Account Data	
Cardholder Data	Sensitive Authentication Data
Primary Account Number (16 digit)	Full Track data (magnetic-stripe data or equivalent on a chip)
Cardholder Name	
Expiration Date	CAV2/CVC2/CVV2/CID
Service Code	PINs/PIN Blocks

3. Scope

3.1. This policy deals with the acceptable use and controls over the receiving, processing and storing of cardholder data across NCG sites.

4. Roles and Responsibilities

4.1. All NCG staff

All staff are legally bound by the rules and principles of the Data Protection Act 2018, the Payment Card Industry (PCI) Data Security Standard v3.2.1 as detailed above in section 2, the EU-GDPR and all other data protection legislation.

All staff shall adhere to all other Group Policies including the Information Security policy, Acceptable Usage Policy and NCG Data Classification Policy.

In addition to the above, there are specific responsibilities for the following groups of people:

4.2. Payment Device Users

NCG Employees responsible for taking card payments and handling sensitive cardholder data shall ensure they:

- Follow the guidelines provided in the payment device manual and the NCG Card Payment Procedure.
- Protect sensitive cardholder data through the secure handling, transportation and disposal of data.
- Do not install unauthorised software or hardware.
- Carry out weekly checks on the payment device to ensure no damage or tampering.
- Submit Incident Report Forms without delay to the relevant person.
- Provide details of changes to personnel responsible for or relocation of payment devices to Group Finance without delay.
- Complete relevant training on card payment security.
- Sign and return procedure, policy and training documents to Group Finance.

4.3. Non Payment Device Users

College Finance are responsible for:

- Maintaining up to date payment device asset register.
- Carrying out regular audit of devices.
- Inform Payment Processor of any changes in location of device.
- Collating policy acceptance and training sign-off forms from payment device users.

Assistant Director – Information Governance is responsible for:

- Annual recertification of NCG PCI compliance.

Information and Data Services are responsible for:

- Maintenance of the IT infrastructure, Network and Firewalls, to support PCI Compliance.
- Installation of PDQ Terminals and, when required, upgrading or replacement of existing terminals.

Group Finance are responsible for:

- Annual Supplier PCI compliance verification.
- Approval of third party suppliers appointed to manage cardholder data.

4.4. PCI Compliance Escalation Team

The Escalation team (Site Security and the Financial Transactions Manager) are responsible for:

- Responding to Incident reports and rectifying any breach of cardholder data and payment device security.
- Escalating incidents to the relevant channels as required – this will be either the College Finance Lead, IT, Governance Team or the Executive Team, depending on the incident.
- Providing support, information and guidance to Payment Device Users as necessary.

5. Protection of Cardholder Data

5.1. Data shall not be recorded, sent or received electronically or written down. Data shall be stored in a secure, locked safe or till when unattended. Paper, merchant copies are to be disposed of securely after the daily bank reconciliation has been completed.

5.2. Staff shall not handle cards, ie cardholders should insert the card into the payment device themselves, with the only exception being cardholders who require assistance through health or disability.

5.3. Data Transportation and Disposal shall be through approved and vetted suppliers who have suitable quality assurance certificates including ISO9001-2008. All suppliers including service providers will be procured through the process as detailed in the NCG Procurement Handbook.

5.4. No technologies shall be added to the cardholder data environment without the explicit approval of Group Finance.

5.5. Staff shall only process cardholder data using approved technologies.

5.6. Staff shall not introduce new technologies to the cardholder data environment.

5.7. NCG allows remote access to technologies to approved vendors/business partners where there is a managed service/contractual agreement in place and only to the specific technologies they require access to and for a specific purpose. Access would be granted via an assigned AD account and use of the RDS Gateway. This would be approved and controlled by the Information and Data Services team.

6. Protection of Assets

6.1. Weekly inspections of payment devices shall be carried out by payment card device users. Checklists are to be completed, signed and saved on the PCI Compliance Teams site by the user as per the NCG Payment Card Procedure.

6.2. All changes in location/user/device shall reported to the PCI Compliance Teams site as per the process detailed in the NCG Payment Card Procedure.

6.3. A register of assets shall be maintained by Group Finance and updated, with an audit trail, when any changes to the inventory is made.

6.4. An annual asset audit shall be carried out by Group Finance and at any other point in time that it is deemed necessary.

6.5. All incidents of damage, tampering, vandalism and substitution shall be reported to the user’s line manager and the PCI Compliance Teams site as per the process detailed in the NCG Payment Card Procedure.

7. Training

7.1. Initial user training will be provided to new users and refresher training will be provided as necessary (and whenever the policy or processes change, or there is a change in legislation or any risks identified.). All staff are responsible for completing the training and uploading signed forms to the PCI Compliance Teams site. All staff are responsible for raising any concerns or requesting additional training for their needs.

8. Linked Policies

- NCG Security Policy.
- NCG Information Security Policy.
- NCG Information Security Incident Reporting Policy.
- NCG Data Classification Policy.
- NCG Acceptable Usage Policy.

9. Linked Procedures

- NCG Card Payment Procedure.
- NCG – Standard Operating Procedure – PCI-DSS Governance.

10. Relevant related Legislation and Standards

- Data protection Act 2018 (DPA 2018).
- Regulation (EU) 2016/679 (General Data Protection Regulation).
- Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1.

Appendix 1

Staff confirmation form

I confirm that I have read and understood the above requirements

Name…………………………………………….

Position…………………………………………..

Department………………………………………

Line Manager……………………………………

Date………………………………………………

Please upload this completed form to the PCI Compliance Teams site