AUDIT COMMITTEE – 24 MARCH 2023

PCI DSS UPDATE

1. RECOMMENDATIONS

1.1 It is recommended that the Audit committee note the contents of this report.

2. INTRODUCTION

2.1 The payment card industry data security standards (PCI DSS) are a set of technical and operational requirements designed to ensure that all organisations that store, process or transmit cardholder data maintain payment security.

2.2 There are 4 PCI DSS compliance levels. New Forest District Council (NFDC) falls into Level 3: for merchants that process 20,000 to 1 million transactions annually. As a Level 3 Merchant NFDC has a requirement to submit a self-assessment questionnaire (SAQ) annually, conduct approved scanning vendor (ASV) scans quarterly and complete the attestation of compliance (AOC) form.

2.3 Non-compliance can lead to termination of the relationship with the bank or an increase in the transaction fees. It can also lead to large fines and penalties.

3. BACKGROUND

3.1 Payment card industry data security standards (PCI DSS) accreditation at NFDC has previously received high priority recommendations through the internal audit plan.

3.2 Terminology & Acronyms

Payment Channels	Different ways customers can make payments to NFDC.
Payment Service Providers (PSP)	Companies that store, process or transmit cardholder data on behalf of another entity.
Third Party Service Providers (TPSP)	Organisations that provide a service/system that has access to the Cardholder Data Environment. As a result, the third party needs to be PCI compliant and provide evidence of this compliance.
Cardholder Data Environment (CDE)	A computer system or network of systems that store, process or transmit cardholder data or sensitive payment authentication data.

3.3 The following table details the payment channels, Payment Service Provider's and Third Party Service Providers' currently utilised at NFDC.

Payment Channel	Payment Service Provider	Third Party Service Provider
Pin Entry Devices (PEDs) • Information offices • Keyhaven River • Car Park Terminals	• Stripe • Worldpay • Till Payments & Allied Irish Bank (AIB)	• Heycentric • None • Parkeon
Telephone Payments • Agent Referred Payments (ARP) taken over the telephone by NFDC personnel • Automated Telephone Payments (ATP) taken using the automated telephone payments system	• Stripe • Opayo & Worldpay	• Sybernet & Heycentric • CivicaPay
Web Payments • Payments taken on the internet	• Stripe	• Heycentric

4. DIFFICULTIES ENCOUNTERED WITH PCI COMPLIANCE

4.1 In January 2022 Mastercard, our Payment Service Provider (PSP), gave notice that they were retiring their payment gateway and therefore withdrawing their services as PSP for NFDC by 31 January 2023.

4.2 Business World, NFDC's Third Party Service Provider (TPSP) for Information Offices, Agent Referred Payments and Web Payments gave notice that they would not be supporting any new PSP's on the existing system and NFDC would need to migrate to a new TPSP, Heycentric.

4.3 The following changes have been implemented as a result of these announcements

i. Card Payments at Information Offices has moved from Mastercard to Stripe as PSP and from Business World to Heycentric as TPSP. This went live on 26th April 2022.

ii. Automated Telephone Payments (ATP) has moved from Mastercard to Opayo as PSP. This went live on 17th October 2022.

iii. Agent Referred Payments (ARP) has moved from Mastercard to Stripe as PSP and from Business World to Heycentric as TPSP. This went live on 26th January 2023.

iv. Web payments has moved from Mastercard to Stripe as PSP and from Business World to Heycentric at TPSP. This went live on 29th November 2022.

4.4 The changes detailed in 4.3 have changed NFDC’s cardholder data environment (CDE) and therefore changed the scope for PCI compliance.

5. PROGRESS MADE TOWARDS PCI DSS COMPLIANCE

5.1 PCI DSS compliance has been validated and confirmed for Car Park Terminals for another year.

5.2 Over the past 12 months we have implemented four new, PCI DSS compliant solutions for taking payments at information offices, Automated Telephone Payments (ATP), Agent Referred Payments (ARP) and Web payments.

5.3 These new solutions work in a way such that no cardholder data ever enters NFDC systems, and all payment details are stored, processed and transmitted by our TPSP and PSP providers.

5.4 The solution providers have demonstrated their compliance by providing copies of their Self-Assessment Questionnaires (SAQs) and Attestation of Compliance (AOC). These will be reviewed and updated annually.

6. NEXT STEPS

6.1 Due to the scale and severity of changes implemented over the past 12 months, the working group will now need to re-map the cardholder data environment (CDE) for all payment channels, to determine which systems and processes fall within the scope of PCI DSS.

6.2 The project team will continue to engage with our bank and third party service providers to obtain appropriate evidence of PCI compliance annually.

6.3 We will use the information obtained from 5.1 & 5.2 to determine which self-assessment questionnaire (SAQ) is required for NFDC.

6.4 We will update our policy and processes to ensure practices are in keeping with PCI compliance. This will include a training package for officers who are involved in the taking of payments to give clarity on the do’s and don’ts when it come to taking payments.

7. FINANCIAL IMPLICATIONS

7.1 There are none

8. CRIME & DISORDER / EQUALITY & DIVERSITY / ENVIRONMENTAL IMPLICATIONS

8.1 There are none

9. DATA PROTECTION IMPLICATIONS

9.1 Any exposure of cardholder data without authorisation is considered a breach for both PCI and GDPR.

For further information contact:

Alan Bethune
Strategic Director Corporate Resources & Transformation
Section 151 Officer
023 8028 5001
Alan.bethune@nfdc.gov.uk

Naomi Baxter
Accountant
023 8028 5033
Naomi.baxter@nfdc.gov.uk