Agenda Item No 4

North East Derbyshire District Council

Cabinet

7 November 2019

PCI-DSS Compliance

Report of Councillor Alex Dale, Deputy Leader and Portfolio Holder for Council Services

Purpose of the Report

- To provide an update to Cabinet of cost and service implications in progressing towards Payment Cards Industry Data Security Standards (PCI-DSS) compliance.
- To recommend and seek approval for measures to facilitate progress towards compliance with the PCI-DSS.

1 Report Details

Background

1.1 The PCI Data Security Standard was originally formed by Visa and MasterCard to bring together their individual compliancy programs. Three other payment brands, American Express, Discover and JCB then joined up which lead to the PCI SSC (Payment Card Industry Security Standards Council) being formed as an independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis.

1.2 The PCI DSS covers the security of all entities that store, process and/or transmit cardholder data including; merchants, processors, acquirers, issuers and service providers as well as all other entities that store, process or transmit cardholder data. The PCI DSS is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This is built upon 12 requirements as shown in the table below; each one consisting of over 240 individual requirements (v3.2).

Control Objectives		Requirements
Build and Maintain a Secure Network	1.	Install and maintain a firewall configuration to protect cardholder data.
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3.	Protect stored cardholder data.
	4.	Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5.	Use and regularly update anti-virus software or programs.
	6.	Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know.
	8.	Assign a unique ID to each person with computer access.
	9.	Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data.
	11.	Regularly test security systems and processes.
Maintain an information Security Policy	12.	Maintain a policy that addresses information security for all personnel.

1.3 A breach of compliance involving the loss of card holder data can result in:

- Significant financial penalties ranging from £1000's to £100,000's, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- In addition, related data breaches enforced by GDPR legislation
- Damage to organisations reputation
- Loss of customer trust

1.4 In order to reduce the scope of PCI and therefore our exposure to risk, the Council should work towards ensuring all risks associated with card payments <u>are reduced as far as is practical.</u>

1.5 A risk management approach must be taken, key elements are:

- Identify all known risks and record them on a risk register
- Develop a risk management program to determine the risk and identify solutions to reduce risk
- Implement / work towards solutions to mitigate the risk
- Continue to monitor and review

The Council operates three different payment channels; e-commerce, card-present and card-not-present. Approximate transactions over a 12 months period break down as follows;

- Telephone transactions is approx. 25,000 per year,

- E-Commerce transactions is approx. 100,000 per year,

- Pin Entry Device transactions is approx. 40,000 per year.

With the total number of transactions being approx. 165,000 per year, the Council is classed as a level 3 merchant which means a self-assessment questionnaire is completed to certify compliance.

1.6 A PCI Working Group (Inc. Rykneld Homes Limited (RHL)) was convened to fully consider the implications to the Council. To date, this group has:

- Commissioned Sec-1 Ltd Security Testing to undertake a gap analysis to identify the key areas to address.
- Received presentations from payment providers to develop understanding possible solutions for card not present payments
- Undertook corporate assessment during 2018 to identifying all non-compliance areas
- Site visits have been undertaken with other Councils to establish how they are addressing compliance.

1.7 At this point in the journey towards compliance there are three key areas that require addressing by the Council:

- Payment Kiosk at Mill Lane
- Risks inherent within the current cardholder not present payment processes Contact Centres and service areas for Capita payments.
- Risks inherent within the current cardholder not present payment processes for Leisure Centre for XN Leisure payments

Payment Kiosk at Mill Lane

1.8 In July, Cabinet approved 'in principle' the removal of the payment kiosk at Mill Lane pending work to encourage alternative payment method. This has been successful and notice has been given through all reasonable means that the kiosk will not be available after 31 December 2019.

1.9 Since Cabinet, a number of things have been done to communicate to customers and service areas that cash payments will no longer be taken at Mill Lane. These include:

- A notice has been placed on the kiosk notifying users that the facility will not be available beyond 3^{t} December and promoting alternative methods of payment.
- Work between the Contact Centre and relevant service areas is ongoing to effectively promote alternative payment options to their customers.
- Social media and The News (December issue) articles to raise awareness and promote alternative payment options.

All of the above will continue up until 31 December however, to date, we have received no complaints from customers or any substantial risks raised by the service areas.

Customer Not Present payments

1.10 Our current telephone payments process for Customer Not Present card payments is currently not PCI-DSS compliant. Currently an officer taking payments must enter the card details on behalf of the customer into our payments solution. To mitigate

risks inherent in this process it is necessary to remove the exposure of the officer from the customer's card details.

1.11 To address the compliance issue a number of options were considered:

1. Capita, our payments solutions provider, have an 'off the shelf' solution called 'Call Secure'. Call Secure is an established solution to 'hand calls off' to an integrated payment line where the customer can input there card details before completing the phone call. The system allows for the Customer Advisor to view that the payment have been inputted, the transaction completed and a reference number generated which is then linked to the enquiry. This solution doesn't provide full PCI compliance due to the data still traversing our (secure) network however, due to our current infrastructure, in particular the analogue telephone lines, this solution is considered to be the best practicably possible solution. Whilst not technically PCI Compliant, a combination of the Call Secure solution and our Public Service Network (PSN) certified approach to cyber security provides a highly mitigated, low risk solution.

   The cost of this solution is an initial **£17k** investment, plus **£12k** per annum licence fee.

2. In addition to 'Call Secure', Capita also provide a solution called 'Call Secure Plus'. This solution is relatively new and to date, there are no other Local Authorities actively using it. Call Secure Plus provides a solution which is PCI Compliant however, to do so requires SIP telephone infrastructure to be so. Following the Mitel Contact Centre upgrade which is currently underway, the transition from analogue to SIP lines is likely to happen in the first half of 2020. Nevertheless, on the basis that this solution is 'untested' with no test sites for us to benchmark against, an additional £10k initial cost and that our current infrastructure would prevent the solution being PCI Compliant, this solution has been discounted at this time.

   The cost of this solution is an initial **£27k** investment, plus **£12k** per annum licence fee.

3. For Leisure a separate payment solution is used which fully integrates with the Leisure Management System, Torrex. This works much the same way as the Capita solution detailed in 1. Despite every effort to obtain details of a solution over the last few months, we are still awaiting a solution and associated costs from XN Leisure. Depending on cost, an alternative solution would be to change working practices and no longer take payments over the phone when booking.

4. An extension of the current Automated Telephone Payments (ATP) solution. Currently, the Council utilise an ATP to take telephone payments for Council Tax. This solution would involve engaging Capita to implement additional payment fund types and some work from ICT, Customer Service and Finance to implement.

   Developing this 'in house' as a solution was given detailed consideration. However, in order to work effectively, the solution required significant changes and additional work from Customer Service Advisors which made the process of collecting and referencing payment less efficient but also less customer friendly. For these reasons, this option was discounted.

However, irrespective of PCI Compliance, this process identified that, in addition to Council Tax, the need for additional ATP's for rents, NNDR, invoices would improve the service by providing more payments options to customers that are more efficient for the Council to administer and accessible to customers outside of office hours. This improvement was purchased in September 2019 and funded from existing budgets.

1.12 Due to the high demand for the PCI solution nationally, Capita have indicated that an installation will not be achievable before March 2020. With this in mind and to limit risk exposure, in consideration of all of the above, the report recommends that the Call Secure solution is implemented as soon as practicably possible. Capita have stated *"We only integrate paye.net and AIM with our own Call Secure solution or Call Secure plus, which uses a Capita partners technology (PCI Pal). We won't integrate with anyone else, so going to tender for this would be a little pointless if I am honest, nobody else can supply the required technology. You would have to replace your whole Corporate Payment management solution and Rykneld Homes's to get a different secure telephone payment system to integrate. Call Secure is simply an upgrade / module to your existing telephone payments solution and would be an addendum to contract, not a whole new contract."*

With this in mind, and following consultation with the Procurement Team, the Exemption to Contract Procedure Rule 4.1(c) should be applied and the Capita quote accepted. 4.1.(c) states: *"The work to be executed or the goods or services to be supplied constitutes an extension to an existing contract and it is the view of the Senior Officer that it would not be in the interest of the service or the Council to tender the contract. The Senior Officer or his or her nominee should consult with the Procurement Service and a record of the decision must be placed on the project file."*

1.13 It should be noted that the above solution will also be applied to RHL. The only other PCI consideration for RHL is the kiosks deployed at Local Area Housing Officers. Due to the age of the kiosks, RHL have been advised that the kiosks are 'out of scope' for a period of 12 months. However, RHL are working with the kiosk provided and are confident existing kiosks can become compliant with upgrades from the supplier.

2 Conclusions and Reasons for Recommendation

2.1 The recommendations seek to provide a practical, economical and risk based solution to PCI DSS compliance, whilst maintaining or enhancing the customer experience and trust in the Council when it comes to personal data.

3 Consultation and Equality Impact

3.1 Consultation has been undertaken with the relevant departments such as ICT, Finance, Customer Services and Rykneld Homes in addition to service areas whose customers regularly use the payment kiosk.

3.2 There are no equality impact considerations directly related to the recommendations in this report.

4 Alternative Options and Reasons for Rejection

a. Do nothing – The do nothing option is not recommended as it would result in failure to address risks outlined in the PCI Standards which could result in loss of customer confidence, reputational damage and in any data breach scenario, exposure to financial penalties and sanctions by the Payment Card Industry Security Standards Council and likely the Information Commissioner through GDPR legislation. However, the risk should not be overstated. The Council has been taking payment card transactions for a number of years without a data breach relating to that information. The PCI Standards seek to mitigate that risk further.

b. All other alternative options have been fully considered in the body of the report.

c. It is important that Cabinet note the recommendation isn't considered to be fully PCI compliant. However, a combination of the Call Secure solution and a high level of cyber security, as certified by PSN, does provide a very low risk solution. To be fully PCI compliant the solution outlined in 1.11(2) should be pursued.

5 Implications

5.1 Finance and Risk Implications

5.1.1 The risk implications are addressed in the body of the report along with 5.2.1 below.

5.1.2 Whilst the recommendations in the report have budget implications, significant savings have been made on Contact Centre budgets in 2019/20. The upgrade of the telephony system from MacFarlane to Mitel delivers a revenue saving of £10k pa and the decision not to replace the kiosk contained in this report creates a saving of £4k pa, through no longer requiring the Security Plus cash collection and changes to the postal process/contract has reduced postal costs in the region of £15k pa. Therefore, the ongoing revenue costs related to the recommendations in this report can be financed through existing Contact Centre budgets whilst still delivering a modest annual saving.

5.1.3 In addition to the risk to the Council, any data breach is likely to present a financial risk to our customers as any loss of data would likely be through criminal activity (Fraud or cyber security attack) in order to obtain data for financial gain.

5.2 Legal Implications including Data Protection

5.2.1 In order to reduce the scope of PCI, organisations should work towards ensuring all risks associated with card payments are reduced as far as is practical.

This report outlines how the Council has taken appropriate steps to mitigate risks associated with PCI Compliance, as for as practicably possible. Further steps will be available to the Council in the future once telephone infrastructure is upgraded to a SIP solution. It should be noted that a breach could result in:

- Significant financial penalties ranging from £1000's to £100,000's, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- In addition, related data breaches enforced by GDPR legislation
- Damage to organisations reputation

- Loss of customer trust

5.2.2 The enforcement of PCI standards is undertaken by the consortium of payment card suppliers that make up the Payment Card Industry Security Standards Council. However, any data breach from the use of payment cards is highly likely to result in a breach in EU GDPR legislation which is enforced by the Information Commissioner. In such circumstances, taking appropriate and proportional action to mitigate risk through achieve PCI Compliance is likely to be a factor in consideration of any penalties.

5.3 Human Resources Implications

5.3.1 There are no human resource implications in relation to these proposals other than the effective use of existing staffing resource. Some changes to working practices will be required during the implementation of the 'customer not present' solutions however, this is considered to be business as usual.

6 Recommendations

6.1 In consideration of paragraph 1.8 and 1.9, Cabinet approve the removal of the non-compliant payment kiosk without replacement.

6.2 That Cabinet approve the budget outlined in 1.11(1) to procure and implement the Call Secure solution for customer not present card payments.

7 Decision Information

Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: *BDC: Revenue - £75,000* ☐ *Capital - £150,000* ☐ *NEDDC: Revenue - £100,000* ☐ *Capital - £250,000* ☐ ☑ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
Has the relevant Portfolio Holder been informed	Yes
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	Transforming how our Council works

8 Document Information

Appendix No	Title
1 2	Kiosk transaction listing by fund Cash transaction figures for the Kiosk
Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
Sec-1 Ltd Report: Cardholder Data Environment Mapping – Oct 18	
Report Author	**Contact Number**
Head of Service Partnerships and Transformation	2210

Payment Method Analysis by Location History
DCO – Mill Lane

T/C – Transaction Count

N/A – Net Amount

(Staff Relocation to DCO 27.04.15)
(BA Payment kiosk installed at DCO on 29.10.2015)

Payment Type Description	Financial Year 2015 /2016 Payment kiosk installed 29.10.2015		Financial Year 2016 / 2017		Financial Year 2017 / 2018		Financial year 2018 / 2019	
	T/C	N/A	T/C	N/A	T/C	N/A	T/C	N/A
Cash	511	£61,000.85	1365	£142,910.22	1174	£143,405.99	980	£120,215.25
Cheques	2468	£966,293.02	5991	£3,575,622.65	5459	£2,271,992.53	3851	£1,695,337.89
Credit Card	39	£5,374.85	79	£12,394.60	51	£13,553.39	76	£24,751.94
Debit Card	144	£21,941.32	584	£85,488.93	585	£93,284.05	548	£108,159.24
Total	3162	£1,054,610.04	8019	£3,816,416.40	7269	£2,522,235.96	5455	£1,948,464.32
Total T/C & N/A Reduction Figures from Previous Years	N/A	N/A	N/A	N/A	750	1,294,180.44	1814	£573,771.64

Appendix 1

* Financial year 2015 / 2016 shows lower as payments are from 29.10.2015 – 31.03.2015 only; the payment kiosk wasn't Installed until 29.10.2015.
* Reduction figure not included for 2016 / 2017 due to not having a full years transactions on previous year (see above note).

Transaction Listing History by Fund
DCO – Mill Lane Payment Kiosk

T/C – Transaction Count

N/A – Net Amount

Financial Year 2018 / 2019

Cash			Cheque		Debit Cards		Credit Card	
Description / Fund Type	**T/C**	**N/A**	**T/C**	**N/A**	**T/C**	**N/A**	**T/C**	**N/A**
Council Tax 02	368	£46,446.87	1871	£481,146.66	218	£49,273.88	11	£4,910.86
Business Rates 04	2	£296.37	229	£258,735.79	4	£1,073.98	0	0
Rykneld Homes Sundry Debtors 05	1	£72.50	0	0	1	£84.00	0	0
Invoices 07	19	£3,298.65	856	£339,410.61	10	£1005.19	3	£1,293.92
Housing Benefit Overpayments 08	57	£2,800.89	102	£18,120.00	15	£9,606.03	1	£19.94
Miscellaneous Payments 09	412	£43,546.60	393	£321,642.30	247	£34,732.62	50	£13,944.46
Land Charges 10	0	0	52	£4,687.00	0	0	0	0

Appendix 2

New Anite Rents 11	109	£22,231.77	24	£5,502.17	35	£7,980.00	2	£2905.76
Housing Water 14	3	£204.20	0	0	3	£343.54	0	0
Planning Admin Fees 21	9	£1,317.40	324	£266,093.36	15	£4060.00	9	£1,677.00
Totals	980	£120,215.25	3851	£1,695,337.89	548	£108,159.24	76	£24,751.94

** Housing Water – no longer applicable – water charges are now paid directly to the water authority