

Management Summary – Update on Progress

What is PCI Compliance?

The major credit card issuers created PCI (Payment Card Industry) compliance standards to protect personal information and ensure security when transactions are processed using a payment card. All members of the payment card industry (financial institutions, credit card companies and merchants) must comply with these standards if they want to accept credit cards. Failure to meet compliance standards can result in fines if personal card data is compromised as well as the loss of the ability to process credit cards. (or more expensive card transaction processing)

What are the PCI DSS requirements?

The PCI DSS standard has 12 requirements for compliance, under the summary headings:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an information security policy

What assessments are required to be performed to prove compliance?

The PCI Data Security Standard establishes four levels based primarily on the volume of transactions processed annually irrespective of acceptance channel. Swindon Borough Council is a level 3 merchant. Level 3 includes merchants who process 20,000 to 6 million transactions a year. The PCI DSS standard requires an annual self-assessment questionnaire be completed with quarterly network vulnerability scans. Onsite assessments and network vulnerability scans are performed by vendors appointed by the card schemes known as Qualified Security Assessor (QSA)

What is Swindon doing to become PCI compliant?

The key IT system to be overhauled is that used for taking payments at the One Stop Shop and the Contact Centre. They are due to be replaced by a system called "Paye.net" before Christmas, and will provide the data security around taking card payments that are necessary to comply with the standard.

Paye.net is effectively software which sits on an internet connected PC, and enables payments to be taken via a "Chip & Pin" machine linked to the PC. In addition, "customer not present" transactions such as when payments are taken over the phone can be processed using Paye.net in a PCI compliant manner.

In addition, all areas of the Council where card payments are taken are under review, and may also utilise Paye.net if this is required as a solution. The major areas that do not require this upgrade are leisure sites who use the "Flex" system as it's already PCI compliant.

PCI training

PCI compliance is also about the policies and procedures in place when staff take payments using debit and credit card. Therefore, all staff that handle card payments have or will receive specific PCI training and a list of “Do’s and Don’ts” will also be circulated and posted on the Councils intranet as a source of information.