Date: 20th January 2017
Enquiries to: Schools' Accountancy Team
Tel: 01473 265626
Email: sat@suffolk.gov.uk

Suffolk County Council

To: All Headteachers and Chairs of Governors of Maintained Schools and PRUs

LMS Document No. 2017/03

Dear Colleagues

Payment Card Industry Data Security Standard (PCI DSS) Compliance and Audit

This letter contains important information for governing bodies/schools and sets out actions that need to be taken.

The Payment Card Industry Data Security Standard (PCI DSS) was introduced to help improve cardholder data security and assist in the uptake of consistent data security measures internationally. Schools should be aware of essential measures that need to be in place if they take card payments via third-party organisations such as ParentPay or handle/process card payments on the school premises.

The Local Authority requires all maintained schools/PRUs to provide an annual assurance that they are compliant with PCI DSS requirements and I am writing today to set out requirements for 2017.

2017 is the third year that schools have been required to complete the PCI DSS Certificate of Compliance, this should be straightforward to complete unless circumstances have changed in your school.

Actions governing bodies and schools need to take:

All maintained schools/PRUs are required to comply with PCI DSS Finance Regulations and complete the 2017 Certificate of PCI DSS Compliance during the spring term. If you are unfamiliar with the requirements then it is essential that you read the Regulations and the information set out in Annex A/A1 of this letter.

- The majority of schools will not need to do anything other than complete Section A of the 2017 Certificate
- Some schools will need to obtain an Attestation of Compliance (or confirm an existing Attestation) and/or complete an annual Self-Assessment Questionnaire. These actions will need to be completed before the Certificate can be completed and schools will need to complete the appropriate section(s) of the 2017 Certificate
- **The 2017 Certificate must be signed by the Headteacher and Chair of Governors**

A copy of the signed Certificate must be sent to sat@suffolk.gov.uk **by 31st March 2017**.

- Copies of Attestation of Compliances and Self-Assessment Questionnaires should not be sent unless requested by the Schools' Accountancy Team

If after reading through the various documents and FAQs you have unanswered queries relating to the processes you have been asked to follow then these should be directed to the Schools' Accountancy Team (sat@suffolk.gov.uk) in the first instance. We recommend that the weekly FAQs issued by Schools' Choice are consulted throughout the year for any further information on PCI DSS.

If there is any significant change to the guidance the Schools' Accountancy Team will write to Headteachers and Chairs of Governors in addition to issuing FAQs.

Yours sincerely

Kirsty Spurgeon
Schools Accountancy Team

Annex A

Who is affected?

Any breach in data security potentially affects the credibility and reputation of individual schools and the Local Authority, as well as exposing individuals to unacceptable risk. Breaches in data can also result in financial penalties which will ultimately fall to the school's Delegated Budget. Governing Bodies should take the issue of data security very seriously and require school staff to comply with PCI DSS requirements at all times.

PCI DSS requirements apply to:

1) All maintained schools/PRUs where credit/debit account data of parents/debtors (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

2) Everyone involved in handling and/or processing payment card processes in schools. This includes staff not directly working in the school but where the accounts operate through the school's Delegated Budget, e.g. a sports centre on school premises.

3) The storage, processing and transmission of cardholder data and the authentication process.

Responsibilities:

PCI DSS Finance Regulations for Suffolk schools set out what schools are required to do and are available to download here Finance Regulations. This LMS Document summarises the main points and sets out the actions that all governing bodies and schools/PRUs now need to take.

Schools are also responsible for ensuring that account/card data is PCI DSS protected by any third-party organisation undertaking payment operations on behalf of the school e.g. ParentPay.

A copy of the PCI DSS standard is available from:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Actions governing bodies and schools need to take:

All schools are now required to complete and submit an annual Certificate of PCI DSS Compliance. We anticipate that the majority of schools will not need to do anything other than complete the annual Certificate; however some schools will also need to obtain an Attestation of Compliance and/or complete an annual Self-Assessment Questionnaire (these actions will need to be completed before the Certificate can be completed).

Annex A1 contains a reference chart to help schools and governors identify the specific action(s) that they will need to take.

The Governing Body is responsible and liable for the protection and security of any payment card information collected, including the use of a PDQ Terminal. This may now be a good opportunity for the school to review whether there is best value from holding a PDQ Terminal and/or taking direct card payments at the school as there is a cost associated with holding Terminals and taking transactions.

Cardholder data (Including 16-digit primary account number, expiry date, 3-digit security code) must never be recorded and/or stored electronically – even for brief periods.

Non-Compliance

If the Local Authority has evidence that a school has failed to comply with the regulations then a Notice of Financial Concern may be issued to place restrictions on governors regarding the collection of further income via payment card methods in order to protect all parties concerned.

Any financial penalties falling to Suffolk County Council as a result of a maintained school/PRU failing to meet PCI DSS requirements will be charged to the school/PRU's Delegated Budget (Sections 6.2.3, 6.2.8, 6.2.11, Scheme for the Financing of Schools)

Support for schools and governors

The PCI DSS requirements set out in this letter may appear daunting at first; however model documents/templates, including a policy and procedures, have been provided to assist schools and governors in drafting the appropriate documents and ensuring that everyone involved knows what is expected of them.

For the majority of schools (i.e. those that do not hold/process card data at the school) there will be minimal work to do and the Schools' Accountancy Team FAQs should answer any queries you may have.

For the remaining small group of schools the process of completing the Self Assessment Questionnaire B for the first time may give rise to questions. The PCI Security Standards Council provides FAQ's (FAQ Knowledge Base) and, if these do not provide the answer that you need, there is the facility within the FAQ Knowledge Base to ask your question(s). The Schools Accountancy Team will not be able to answer queries on specific questions within the Questionnaire.

- We recommend that the Policy and Procedures are introduced as soon as practical; the Self Assessment Questionnaire may then be completed at a later date, provided it is done by *31 March 2017*

- A model Policy and model Procedure can be downloaded from the Schools' Choice website, Staff Declaration and Staff Log templates are also available

Annex A1

SUMMARY OF ACTIONS SCHOOLS NEED TO TAKE:

The school ……	Action Needed
- doesn't use a third-party organisation (e.g. ParentPay) - **AND** doesn't accept/process card payments and has no stored account data	- **Complete Section A** of the Certificate and send to sat@suffolk.gov.uk by *31 March 2017*
- uses a third-party organisation (e.g. ParentPay) - **BUT** doesn't accept/process card payments and has no stored account data	- **Complete Section B** of the Certificate and send to sat@suffolk.gov.uk by *31 March 2017* - Obtain an Attestation of Compliance from the third-party organisation. These are usually published on their websites (annual task) - Complete the PCI DSS section of the RoFR
- does one or more of the following: a) holds a PDQ Terminal b) handles/processes account/card data c) holds account/card data - **BUT** doesn't use a third-party organisation (e.g. ParentPay)	- **Complete Section C** of the Certificate and send to sat@suffolk.gov.uk by *31 March 2017* - Agree a PCI DSS Policy and arrange for regular reviews (model policy available) - Identify appropriate procedures and add written instructions to the school's Local Procedures Manual (model procedures available) - Complete the PCI DSS Self Assessment Questionnaire B, the signed copy is retained in school (annual task) - Complete the PCI DSS section of the RoFR
- does one or more of the following: a) holds a PDQ Terminal b) handles/processes account/card data c) holds account/card data - **AND** uses a third-party organisation (e.g. ParentPay)	- **Complete Section B AND Section C** of the Certificate and send to sat@suffolk.gov.uk by *31 March 2017* - Obtain an Attestation of Compliance from the third-party organisation. These are usually published on their websites (annual task) - Agree a PCI DSS Policy and arrange for regular reviews (model policy available) - Identify appropriate procedures and add written instructions to the school's Local Procedures Manual (model procedures available) - Complete the PCI DSS Self Assessment Questionnaire B, the signed copy is retained in school – annual task - Complete the PCI DSS section of the RoFR