**Schools’ Accountancy Team**

Finance Regulations

This document should be used in conjunction with the [Suffolk Scheme for the Financing of Schools.](http://www.suffolklearning.co.uk/leadership-staff-development/schools-accountancy/finance-regulations)

SECTION 5.5: ADMINISTRATIVE PROCEDURES FOR THE COLLECTION OF INCOME

PCI DSS AND CREDIT/DEBIT CARD HANDLING

**Payment Card Industry Data Security Standard (PCI DSS)**

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.

PCI DSS requirements apply to:

* all maintained schools/PRUs where credit/debit account data of parents/debtors (cardholder data and/or sensitive authentication data) is stored, processed or transmitted
* everyone involved in 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
* the storage, processing and transmission of cardholder data and the authentication process

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.

Any breach in data security potentially affects the credibility and reputation of individual schools and 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.

A copy of the PCI DSS standard is available from:

<https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml>

**Governing Body Responsibilities**

**PCI DSS Policy**

Where credit/debit card payments are to be accepted/processed directly by the school, or where they have been in the past and the associated records are still held:

* the Governing Body should agree delegation arrangements for the introduction and subsequent regular reviews of a PCI DSS Policy

**Third-Party Organisations – Attestation of Compliance**

Where third-party organisations are undertaking payment operations on behalf of the school (e.g. ParentPay), even if direct payments are not accepted by the school:

* the school should obtain an Attestation of Compliance document from each third-party organisation and the Governing Body should specify in the Record of Financial Responsibility (RoFR) who is responsible for doing this.

**Protection and security**

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.

Day-to-day management should be delegated to the Headteacher/Business Manager who should arrange for written instructions to be included in the school’s Local Procedures Manual.

The Governing Body should require that school staff ensure:

* all staff to be made aware of the PCI DSS Policy and Procedures when it is first introduced; or upon taking up an appointment with the school at a later date, and are to sign as evidence that this has been done. This is to ensure that non-authorised staff are aware that they must not handle card data.
* all staff using the Terminal and/or handling data are to be regularly reminded of the governors’ Policy and the school’s Local Procedures on payment card processing. They should sign an annual declaration to confirm this;
* all staff authorised to handle card information must undertake PCI DSS training recommended by the Local Authority
* secure storage of the Terminal when not in use;
* secure handling and storage of the merchant transaction slips;
* secure destruction of the merchant transaction slips when no longer required (maximum 6 months from the date). N.B. a Category 4 (2mm x 2mm cross cut) shredder is an acceptable means of destruction/disposal;
* regular inspection of the Terminal to ensure it has not been tampered with or swapped;
* Certificates of PCI DSS Compliance are submitted to the Local Authority annually within specified deadlines
* Completed Self-Assessment Questionnaires are completed annually and retained in school. Questionnaires should be submitted to the Local Authority promptly upon request

These requirements should be included in the school PCI DSS Policy.

***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.***

***Schools using VOIP telephone systems must not take card details over the phone.***

Appropriate entries must be made and reconciled promptly on FMS for incomes collected via payment card methods, in line with general financial regulations relating to income.

This is not an exhaustive set of requirements, further requirements may be issued via LMS Documents and it is the school’s responsibility to ensure that PCI DSS requirements are met.

**Evidence of Compliance to PCI DSS**

**Certificate of PCI DSS Compliance**

All maintained schools and PRUs must complete an annual Certificate of PCI DSS Compliance and send a signed copy to the Local Authority by the specified deadlines each year.

**Attestation of Compliance**

Where third-party organisations are undertaking payment operations on behalf of the school (e.g. ParentPay) the school should obtain an Attestation of Compliance from each third-party organisation.

**Self Assessment Questionnaire**

The PCI DSS [Self Assessment Questionnaire B](https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B.pdf?agreement=true&time=1548415465604) will need to be completed annually by schools where credit/debit account data of parents/debtors (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. The Chair of Governors must sign the completed Questionnaire which is retained by the school.

A copy of the signed Self Assessment Questionnaire must be provided to the Local Authority upon request.

Governors need to put in place an appropriate action plan to address any weaknesses identified by the Questionnaire and monitor progress until the school is fully compliant. The actions should be completed before the next annual completion of the Self-Assessment Questionnaire is due.

**PCI DSS School File**

It is recommended that schools which accept/process card payments maintain a PCI DSS file to include:

* The school’s current PCI DSS Policy
* The school’s current Payment Card Handling Procedures
* The PDQ Terminal operating manual and ‘short-cut’ guide
* Evidence that all staff have had access to the school’s PCI DSS Policy and Procedures e.g. PCI DSS Staff Log
* Signed declarations from all members of staff authorised to handle payment card data (including 16-digit primary account number, expiry date, 3-digit security code) and/or PDQ Terminals
* Log of visual inspections of PDQ Terminal
* Completed, signed PCI DSS Self-Assessment Questionnaires
* Signed Certificate of PCI DSS Compliance
* A copy of these Finance Regulations and copies of appropriate LMS Documents and FAQs

Staff should be aware of where to find the file and any appropriate documents not located in the file.

**Audit**

Suffolk County Council Internal or External Auditors may audit the School to confirm PCI DSS compliance; the audit(s) may be carried out by a PCI DSS Qualified Security Assessor. Schools are required to co-operate with auditors (*Section 2.6 Scheme for the Financing of Schools*).

**Non-Compliance**

If the Local Authority has evidence that a school has failed to comply with these 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*)

HELP AND ADVICE

SCHOOLS’ ACCOUNTANCY TEAM

Statutory and compliance queries should be raised with the Schools’ Accountancy Team:

* sat@suffolk.gov.uk
* Tel: 01473 265626
* Schools’ Accountancy Team, Floor 3, Constantine House, 5 Constantine Road, Ipswich, Suffolk, IP1 2DH

SCHOOLS’ CHOICE

Help and support on implementing the Finance Regulations is available from Schools’ Choice:

Finance Helpline:

* finance@schoolschoice.org
* Tel: 0345 603 7684
* Schools’ Choice, Endeavour House, 8 Russell Road, Ipswich, Suffolk, IP1 2BX

Enhanced Finance Service:

* efs@schoolschoice.org
* Tel: 01473 264054

This document should be used in conjunction with the [Suffolk Scheme for the Financing of Schools](https://www.schoolsurf.suffolkcc.gov.uk/docs/unrestricted/LMS/Consultation/FINAL%20_SCHEME.doc).

Kirsty Spurgeon

Schools Accountancy Team

Version: January 2019

We will on request produce this document, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.