

**………………………….SCHOOL**

**PAYMENT CARD INDUSTRY**

**DATA SECURITY STANDARD**

**(PCI DSS) POLICY**

|  |  |  |
| --- | --- | --- |
| **DELEGATION OF APPROVAL TO:** |  | **COMMITTEE** |
| **FREQUENCY OF REVIEWS:** | ***Annually*** |
|  |  |
| **DATE APPROVED:** |  |
| **COMMITTEE CHAIR:** |  |
| **CHAIR OF GOVERNORS:** |  |
| **DATE RECEIVED BY WGB:** |  |
|  |  |
| **DATE NEXT REVIEW DUE:** |  |

**POLICY OVERVIEW**

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 the School whilst account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.
* PCI DSS applies to everyone involved in payment card processes in the School, including the storage, processing and transmission of cardholder data and the authentication process.
* The School is responsible for ensuring that account 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 the school as well as exposing individuals to unacceptable risk. Therefore the Governing Body takes the issue of data security very seriously and requires School Staff to comply with the appropriate Policy and Local Procedure requirements at all times.

**COMPLIANCE TO PCI DSS**

As a maintained school and a holder of a PDQ Terminal the School is required by its Merchant Acquirer (*insert name of Merchant Acquirer)* and Suffolk County Councilto be continuously compliant with the current version of the PCI DSS.

A copy of this standard is available from:

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

The Governing Body accepts full responsibility and liability for the protection and security of any payment card information collected whilst using the PDQ Terminal. The Governing Body requires School Staff to 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

This is not an exhaustive set of requirements and it is the School’s responsibility to ensure that PCI DSS requirements are met.

**EVIDENCE OF COMPLIANCE TO PCI DSS**

Compliance to PCI DSS by the School will be acknowledged by the completion of the PCI DSS [Self Assessment Questionnaire B](https://listings.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-B-rev1_1.pdf) signed by the School’s Chair of Governors annually. An Action Plan to address any weaknesses identified will be drawn up and progress will be monitored by *Finance Committee or Full Governing Body* until fully compliant. A copy of the completed Questionnaire will be forwarded to the Local Authority upon request.

The School will complete an annual Certificate of PCI DSS Compliance and send a signed copy to the Local Authority by the specified deadlines each year.

The Governing Body is aware that 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.