GUIDANCE FOR SCHOOLS AND PARENT TEACHER ASSOCIATIONS

DATA PROTECTION (UK GDPR) AND PCI DSS COMPLIANCE

1. Purpose of this Guidance

This document has been developed to provide clarification and practical guidance to schools, governors

and Parent Teacher Associations (PTAs) regarding their respective responsibilities when handling personal data and accepting payment card transactions.

Whilst PTAs are generally independent charitable organisations, there is often a perceived association between PTAs, schools, and the Council. It is therefore important that appropriate standards of data protection and payment security are maintained.

This guidance relates to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Payment Card Industry Data Security Standard (PCI DSS)

2. Status of PTAs

PTAs are typically:

- Independent charities
- Separate legal entities from the school
- Their own Data Controllers under UK GDPR

As Data Controllers, PTAs are responsible for determining how personal data is processed and for demonstrating compliance with data protection legislation.

In addition, where PTAs accept debit and credit card payments, PCI DSS compliance forms part of their contractual obligations with their payment provider and acquiring bank. As well as providing the citizens they serve the assurance for their financial details remain safe.

The Information Commissioner's Office guidance makes it clear that organisations handling debit and credit card payments must implement appropriate security measures in line with data protection obligations.

Cardiff Council cannot approve or authorise specific payment devices, providers, or platforms. Responsibility for compliance rests directly with the PTA, whilst they take debit and credit card payments.

3. PCI DSS – Practical Compliance Requirements

Where PTAs accept debit and credit card payments (using either chip and pin devices or online platforms), the following PCI controls should be considered.

3.1 Chip and Pin Devices

PTAs should ensure that:

- The supplier of the device has been validated as PCI compliant.
- A process exists to confirm the supplier maintains their PCI compliance on an annual basis.
- Evidence of the device's compliance has been obtained via the Payment Card Industry Security Standards Council (PCI SSC) website.
- A Self-Assessment Questionnaire (SAQ) has been completed where the PTA uses its own Merchant ID (MID).
- Individuals using devices have received basic training in:
    - Secure handling of devices
    - Recognising signs of tampering
- Regular checks are undertaken to identify tampering, and these checks are recorded.
- Merchant receipts are stored securely and retained in accordance with Mastercard retention requirements (currently five years). Note that,
    - It is essential that the receipts do not display the full Primary Account Number (PAN). Only the first six and last four digits should be visible.
    - Receipts must be reviewed every quarter and when they have reached their retention period disposed of securely (e.g. cross-cut shredding or confidential waste disposal).

3.2 E-Payments and Online Payment Platforms

Where online or remote debit and credit card payments are accepted, PTAs should ensure:

- The payment provider is PCI compliant.
- PCI compliance is reviewed and validated annually.
- Documentary evidence of compliance is obtained (e.g. confirmation of Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AOC) has been completed).
- The PTA completes its own SAQ where operating under its own Merchant ID (MID).

4. Data Protection (UK GDPR) Responsibilities

In addition to PCI DSS obligations, PTAs must comply with UK GDPR and the Data Protection Act 2018.

This includes:

- Collecting only personal data that is necessary for the stated purpose.
- Ensuring personal data is processed lawfully, fairly, and transparently.
- Implementing appropriate technical and organisational security measures.
- Restricting access to authorised volunteers.
- Retaining information only for as long as necessary.
- Providing appropriate privacy information to individuals.
- Examples of personal data processed by PTAs may include:
- Parent and pupil contact details
- Donor information
- Volunteer details
- Event registration information

Failure to implement appropriate safeguards may expose the PTA to regulatory risk and reputational harm. As noted above, there is often a perceived association between PTAs, schools, and the Council and so this may also present risks to these organisations too.

5. Role of Schools

Schools have the best knowledge and relationship with PTAs and are requested to:

- Share this guidance with their PTA or equivalent fundraising body.
- Ensure PTAs understand their independent Data Controller responsibilities.
- Gain assurance that PTAs understand their responsibilities when taking debit and credit card payments
- Encourage PTAs to seek independent advice where necessary in relation to their legal and contractual obligations.

Contact Details

Natalie Blackler
Information Governance School Support Officer
Telephone — 07974842771
Email— Dataprotectionschools@cardiff.gov.uk