

Information Security Policy: Online Payment Processing

Associated Board of Dance LTD

Information Security Policy: Online Payment Processing

Date: 2025-05-06

1. Purpose

This policy outlines the security practices and responsibilities related to the handling of online payments, ensuring the protection of customer data and compliance with PCI DSS and GDPR.

2. Scope

This policy applies to all office staff at Associated Board of Dance LTD who have access to systems and services related to the processing of online orders and payment redirection.

3. Payment Processing Overview

- All online payments are securely handled through PayPal, including both credit/debit card transactions and PayPal accounts.
- In-person payments at select events are processed via Zettle by PayPal card readers.
- Associated Board of Dance LTD does not collect, process, or store any cardholder data directly.
- The online store is powered by WHMCS, which is configured to redirect all payment activity to PayPal's secure platform.

4. Data Protection and GDPR Compliance

- We collect and store only essential contact information for members and customers (e.g., name, email, postal address).
- No payment details are ever stored, transmitted, or viewed by any staff.
- All personal data is handled in accordance with GDPR requirements and our internal Privacy Policy.

5. PCI Compliance

- As payment data is entirely handled through third-party PCI-compliant services (PayPal/Zettle), we

maintain our compliance through:

- Ensuring no storage or processing of card data on our systems
- Keeping software and plugins up to date
- Maintaining secure configuration of our WHMCS platform
- Completing PCI self-assessment questionnaires as required

6. Staff Responsibilities

- Staff must never request, receive, or record card payment details from customers.
- Staff must report any suspected security incident, data breach, or phishing attempt immediately to management.
- WHMCS admin and PayPal access credentials must be strong, unique, and never shared.
- Devices used for payment-related activities must have updated antivirus software and system security patches.

7. System Access & Security

- Access to the WHMCS system is restricted to authorised staff via secure login credentials.
- Access logs are monitored regularly.
- All staff are required to use strong passwords and change them regularly.

8. Event Payments (Zettle by PayPal)

- Devices used with Zettle are kept secure and only operated by trained staff.
- Payment data is processed directly via Zettle's encrypted system and never accessed by Associated Board of Dance LTD.

9. Review & Updates

This policy is reviewed annually or upon any major change to payment processing methods, platforms, or regulations.