Australian Chiropractic College

POLICY AND PROCEDURE

MANAGING SPONSORSHIP/SUPPORTER/STUDENT CREDIT/DEBIT CARD DATA

1. OVERVIEW

The use of credit or debit cards (payment cards) by Australian Chiropractic College Limited ('ACC', 'College') sponsors, supporters and students are done so via the adoption of efficient business practices and benefits those making donations and payments to the College.

The College and its third party service providers are committed to protecting sponsor/supporter/student payment card data and preserving card provider relationships through compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Failure by the College or its service providers to comply with the PCI DSS may result in substantial fines, loss of the ability to accept payment cards, increased auditing, liability for fraudulent transactions, and damage to the College's reputation.

The College adopts generally accepted systems and procedures supporting its Financial Management and related Invoicing and Cash Receipting processes, along with relevant outsourcing to experts its risk management of Technology Services inclusive of Identity and Access Management.

2. SCOPE AND APPLICATION

This document and procedures apply across the College to all staff and their supervisors who:

a) handle or process payment card information or card transactions; or
b) are in a position where they may monitor or approve payment card information or requests for such information.

3. PROCEDURES

These procedures are based on the general principle that staff must only accept, transmit, use, retain and destroy payment card account data in a manner which protects the data from misuse or from unauthorised transactions.

A. Payment card processing

Responsibility: College professional staff members:

a) Ensure that all payments to the College received by payment card are processed by a College-approved PCI DSS-compliant third party internet gateway (e.g., any of the College's eCommerce online sales solutions) or an EFTPOS machine approved by the Corporate Services Manager in accordance with the Invoicing and Cash Receipting Procedures. (Only EFTPOS machines supplied and owned by the College aligned banking institution will be approved).
b) Ensure that procedures are in place for all EFTPOS machines to be stored securely when not in use (e.g., when unattended or overnight).
c) Ensure that procedures are in place to verify weekly that EFTPOS machines have not been tampered with.

Responsibility: Staff authorised to receive payments at Cash Receipting Locations:

d) If payments are made when the card is **present** (i.e., usually because the cardholder is present in person), process the payment directly on an EFTPOS machine, and not via any other mechanism.
e) If payments are made via **telephone** without the physical card, key the cardholder data received (PAN, expiry date and CCV) directly into the EFTPOS machine and do not write it down. If the data is written down, or captured in any form of voice recording, destroy or delete it without delay when the transaction is processed: see Procedure B.f).
f) If payment is received via a **dedicated analogue fax line**, key the cardholder data into an EFTPOS machine immediately on receipt of the paper fax, and destroy the fax without delay when the transaction is processed: see Procedure B.f). Physical access to the fax machine must be restricted (e.g., in a locked cabinet or locked room) to staff who meet the requirements of Procedure C.
g) Do **not** accept or transmit payment details via an **email,** an **instant message,** a **facsimile on a multi-function device,** or a **VoIP fax**, as these forms of transmission are not secure. If an email, instant message or non-complying facsimile is received from an account payer with their PAN:
    i. Reply immediately – with the PAN deleted – with the statement "*Your transaction has not been processed. To better protect your identity, the College cannot accept your credit card number over email or facsimile as it is not a secure method of receiving and transmitting cardholder data. Please use an approved method such as telephone, mail, in-person or an online option (if applicable)*."
    ii. Ensure the email is deleted and the trash folder emptied; or the instant message is deleted; or the facsimile is securely destroyed: see Procedure B.f).

B. Storing and destroying cardholder data

Responsibility: Any staff member with access to cardholder data

a) Do not store cardholder data (PAN, cardholder name and expiry date with the exception of CCV) unless there is a legitimate business need (e.g., chargeback or refunds) AND a documented storage procedure is approved by the Chief Financial Officer and/or the Manager, Risk & Security.
b) Once a transaction has been processed, do not store or record CCV numbers under any circumstances. Never store other sensitive authentication data, such as data on the magnetic stripe or chip and PINs. (*The College is required to comply with State and Commonwealth legislation related to recordkeeping).*
c) Destroy cardholder data as soon as the business need for the storage is no longer relevant, or within six months of the date of the transaction, whichever is shorter. (*The College is required to comply with State and Commonwealth legislation related to recordkeeping).*

d) Only store the first six and last four digits of a cardholder PAN, the cardholder name and card expiry date. Overwriting the numbers with a marker or white out or black tape is not acceptable. The best option is to cut the numbers from the document. The time, date, transaction identification and amount may be stored.
e) Ensure any cardholder data in **hard copy** retained under Procedure B.a. is stored in a secure and protected manner within a locked filing cabinet or safe within a locked office; and that access is restricted to staff with a legitimate business need for such data.
f) To destroy **hard copy** cardholder data, use at least one of the following methods: cross cut shredding, incinerating, or a secure disposal service. (For further information on ways to securely destroy cardholder data, including advice on the design of payment forms so that the relevant data can be easily removed, contact the College's Corporate Services Department responsible for PCI DSS Compliance).
g) Do not store cardholder data on spreadsheets, in College receipt books, on TRIM (document management system) or in any removable storage medium such as DVDs, CDs or USB flash drives.
h) Do not store, process or transmit **electronic** cardholder data on College computers (including laptops, tablets or smartphones, hard drive of any computer servers or network storage devices) in any form (including scanning into TRIM), unless an exception has been approved by the Corporate Services Manager and a documented procedure has been put in place.

C. Staff access to cardholder data and training

Responsibility: College Professional Staff:

a) Ensure that only staff with a legitimate business need for cardholder data are provided with access to such data;
b) Ensure that training in payment card processing and the PCI DSS is successfully completed before any staff member is permitted to process payment card payments, and that training is successfully completed annually thereafter;
c) Ensure that all staff with access to cardholder data have signed an acknowledgement that they understand and will comply with these procedures before being given access to cardholder data; and
d) Ensure that a record of all training and the signed acknowledgements is maintained.

D. Secure data transmittal

Responsibility: All staff with access to cardholder data:

a) Ensure that cardholder data is not transmitted unless the means of transmittal is secure. In general, the only secure method for intra-College cardholder data transmittal is hand delivery or telephone (voice recordings must be deleted without delay when the transaction is processed);
b) Ensure that no cardholder data is emailed, or transmitted as an instant message or text message.

E. Ensure that no cardholder data is faxed, either internally or externally between staff or sponsors/students, unless both the sending and receiving facsimile machines are directly linked to an analogue line specifically installed for this purpose. PCI DSS compliance by service providers and third party vendors.

All service providers and third party vendors providing payment card related services for the College must:

- be PCI DSS compliant;
- acknowledge in writing their responsibility for the security of cardholder data in their possession; and
- provide an annual Attestation of Compliance that the version of the vendor's system and procedures used by The College of Adelaide are PCI-DSS compliant.

Responsibility: Any staff engaged in negotiation with service providers and third party vendors for payment card related services:

a) Ensure that all service providers and third party vendors are PCI DSS compliant, or are assessed and approved by Corporate Services with respect to PCI compliance, before any agreement to provide services is concluded;
b) Ensure that all agreements with service providers and third party vendors include a provision that the service provider or third party vendor will protect cardholder data in accordance with the PCI DSS requirements;
c) Ensure that all service providers and third party vendors have their PCI DSS compliance reviewed annually.

Examples of service providers or third party vendors who provide services to the College include:

- NAB ecommerce payment gateway; and
- *Blackbaud eTapestry (eTap)* fundraising management platform.

F. Monitoring and review

a) The Corporate Services Manager and/or the College IT Service Provider may arrange random audits for all College business areas in order to verify compliance with these procedures; and
b) Any payment card data storage in contravention of this procedure will be reported to the Manager, Risk & Security, in Technology Services, immediately, who will ensure that the data is removed in accordance with these procedures and the PCI DSS.

G. Responsibilities

a) College Professional Staff are responsible for:

- ensuring that all card payment processes and systems within the College are compliant with these procedures;
- allocating responsibilities to suitable staff within the College under these procedures; and
- reviewing compliance with these procedures within the College at least annually.

b) The College's Corporate Services Manager and PCI DSS Compliance Officer and IT Service provider pertaining to Risk & Security in Technology Services are collectively responsible for completing its self-assessment on behalf of the College and for coordinating responses to suspected or actual breaches in security of payment card data;
c) The College's Corporate Services Manager and PCI DSS Compliance Office is responsible for monitoring PCI compliance and co-ordinating annual College Review of PCI Compliance.
d) The College's Accounts Payable unit, in Corporate Services or external Bookkeeper is responsible for the annual review and update of the Merchant Facilities (EFTPOS) register to facilitate review and monitoring of compliance with these procedures.

H. IT Controls

Responsibility: Corporate Services Manager

a) Maintain a documented list of assets, collectively referred to as cardholder data environment (CDE), including servers, network devices and end points, that are considered "in scope" for compliance with PCI DSS, as well as a network diagram describing the flow of cardholder data.
b) Ensure that necessary policies and standards as required by PCI DSS are developed, maintained and promulgated to staff responsible for the maintenance of assets that reside within the College CDE.
c) Ensure that technical controls as required by PCI DSS are in place for all assets within the College CDE. Where it is not practical to implement required controls, then mitigating controls must be considered and developed.

4. DEFINITIONS

Review/Attestation of Compliance: A declaration by an organisation that handles payment card data (i.e. a service provider or third party vendor) that it is compliant with PCI DSS requirements.
CCV: The Credit Card Verification number on each payment card, as follows:
CVC2: Card Verification Code (MasterCard) on signature panel
CVV2: Card Verification Value (Visa) on signature panel
CID: Card Identification number (American Express) above logo on front of card.
Cardholder Data: Data consisting of the full PAN, or data in the form of the full PAN and any of the following: cardholder name, expiration date and/or the CCV number.
CDE: Cardholder Data Environment: a computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component that directly connects to or supports this network.
EFTPOS: Electronic Funds Transfer Point of Sale. The College may use a variety of EFTPOS machines that accept American Express, MasterCard and Visa payment cards. These are sometimes referred to as Merchant Facilities.
Instant message: Any form of online chat which offers real-time text transmission over the internet.
Multi-function device: A network-connected printer/scanner/copier/facsimile machine.
PAN: Primary Account Number: the unique payment card number that identifies the issuer and the particular cardholder account.
PCI DSS: Payment Card Industry Data Security Standards**:** a security standard with a set of requirements that must be followed by organisations that handle (accept, transmit, store) payment card data.
SAQ: Self-Assessment Questionnaire: Reporting tool used to document self-assessment results from the College's PCI DSS assessment.
Service providers and third party vendors: Any organisation that processes, transmits or stores cardholder data on behalf of The College.
VoIP: Voice-over-Internet Protocol, i.e., communication received via the internet.