Association of Christian Teachers (ACT)

www.christians-in-education.org.uk

Electronic Transactions Security Policy

(Originally posted: 1 November 2008 / Last updated: 1 March 2009)

1 VISION AND PURPOSE

1.1 ACT aims to be an active, confident and secure participant in the global digital economy.

1.2 The purpose of this ***Electronic Transactions Security Policy*** is to define the guidelines for accepting and processing credit cards and debit cards and storing personal cardholder information. This policy will help to ensure that cardholder information supplied to ACT is secure and protected.

2 SCOPE

2.1 This policy applies to all ACT paid employees, volunteers and representatives of the Association. The policy pertains to all departments that process, transmit or handle cardholder information – whether in a physical or an electronic format.

3 PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

3.1 ACT's website and ***Electronic Transactions Security Policy*** conform with credit/debit card company requirements and adhere to Payment Card Industry (PCI) Data Security Standards (DSS).

3.2 The ACT Office Manager is responsible for carrying out an annual self-audit of the ACT website and ***Electronic Transactions Security Policy*** to ensure they conform with credit credit/debit card company requirements and adhere to Payment Card Industry (PCI) Data Security Standards (DSS).

4 POLICY

4.1 All transactions that ACT processes must meet the standards outlined in this policy. All ACT paid employees, volunteers and representatives of the Association must comply with the Payment Card Industry Data Security Standards.

4.2 Strict control is maintained over the storage, accessibility and internal or external distribution of any kind of media, whether paper and electronic, that contains cardholder data.

4.3 All paper and electronic cardholder data is to be classified and identified as confidential.

4.4 All paper and electronic cardholder data must be locked in a physically secure area.

4.5 Prior approval from the ACT Office Manager must be obtained before any and all cardholder information can be moved from a secured area.

4.6 Access to computing resources and cardholder information is limited to only those individuals whose jobs require such access, on a strict 'need to know' basis.

4.7 Electronic credit card and debit card numbers must not be transmitted or stored on a personal computer or email account. Electronic lists of customers' card numbers should not be retained.

4.8 In accordance with ACT's ***Electronic Transactions Security Policy*** and ***Privacy Policy***, any cardholder information sent by electronic means will first be encrypted using industry standard technology for secure commercial transactions. If cardholder information is sent by physical means (e.g. via a secure courier) steps will be taken to ensure that it can be accurately tracked en route.

4.9 Credit card and debit card information should only be accepted by ACT online, by telephone, mail or in person. Credit/debit card information will not be accepted via email and ACT paid employees, volunteers and representatives must not email credit/debit card information.

4.10 Only essential information should be stored. ACT will not store the Card Validation Code (also known as the Security Digits, V Code, or CID). ACT will not store users' PINs or the full data from a card's magnetic stripe.

4.11 Credit card and debit card information should only be retained for the time needed to process, or if retained for business or legal reasons, for as long as necessary.

4.12 Hardcopies of credit card and debit card information, if it does not need to be retained, should be destroyed (i.e. cross-cut shredded, incinerated, or pulped) immediately after processing, or immediately after the information no longer needs to be retained.

4.13 Credit card and debit card receipts may only show up to the last five digits of the card number. If receipts show more than the last five digits, the receipts must be retained in a secure area (see 4.3 and 4.4) or destroyed (see 4.12).

5 OVERSIGHT AND MANAGEMENT OF PROCEDURES

5.1 All credit card and debit card transaction acceptance, including web-based transactions, should be initiated and controlled by the ACT Office Manager.

5.2 The ACT Office Manager is responsible for ensuring that the safeguards and procedures outlined in ACT's ***Electronic Transactions Security Policy*** and ***Privacy Policy*** are executed.

5.3 As part of a formal security awareness programme, all ACT employees and Trustees/Directors of the Association should be involved in a review of ACT's ***Electronic Transactions Security Policy*** at least once a year in the light of recent legal/technological/commercial developments in terms of 'best practice'.

5.4 The ACT Office Manager is responsible for clearly explaining security responsibilities for all employees and contractors and ensuring they receive a copy of ACT's ***Electronic Transactions Security Policy***.

5.5 The ACT Office Manager should define and manage the proper use of critical employee-facing technologies (such as modems and wireless) for all employees and contractors, in line with ACT's ***Electronic Transactions Security Policy*** and ***Privacy Policy***.

5.6 In conjunction with ACT's Treasurer the ACT Office Manager should establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

5.7 If cardholder data is shared with service providers then: (a) the service provider must demonstrate adherence to PCI DSS requirements; and (b) the service provider must acknowledge that they are responsible for the security of any and all cardholder data in their possession.