OUTLET QUICK REFERENCE PCI-DSS PROCEDURES

In order to comply with Payment Card Industry Data Security Standards (PCI-DSS) as well as good business practices related to the handling of credit/debit card information the following should be established in each of the outlets/schools/services that use and take credit/debit card payments either in person (Cardholder present), or over the telephone (Cardholder not present):

Data Handling

- Credit /Debit Card Holder details (CHD) data must be treated as confidential at all times
- Data that is not absolutely necessary in order to conduct business must not be retained in any format (e.g., paper or electronic).
- Do not accept, request, or retain such data via e-mail or other electronic means.(should a student, customer send their details in this way the details can be used, the email etc. should be deleted and IT helpdesk contacted and the person contacted to advise that they we will not accept payment in this way. **Please note** do not use the "Reply" as this may inappropriately transmit credit card information.
- Do not write down or store any card-validation code (i.e., the three- or four-digit code) used to validate a card-not-present transaction, personal identification number (PIN) or encrypted PIN block.
- Account numbers will be masked if and when displayed (i.e., no more than the first six and last four digits of the credit card numbers).
- Cash Services are to be contacted regarding any PDQ (card machines) are placed into service without their assistance.
- The serial numbers on PDQ's must be checked and validated regularly.
- PDQ's must not be left unattended at any time and secured at the end of business
- Physical access to CHD will be restricted to staff with a "business-need-to-know" and should be locked securely. Means such as locked file cabinets and restricted file rooms as well as restricted distribution of such records will be used.
- If external media or couriers are used to transmit or transfer such data, we will use means that enable tracking of the data. Any transfer using these, or similar means will be approved by appropriate levels of management before the fact.
- CHD should only be retained for a maximum of 2 months after this period of time, the data needs to be shredded using a cross-cut shredder or otherwise dispose of this information in a PCI-DSS approved manner.

Processing Refunds

- Refunds can be made but only back to the card the original payments were collected from and must be authorised by a senior member of staff (please contact Cash Services if you require any assistance of information regarding refunds).

These procedures apply to all processes, and personnel that relate to the processing of Debt/Credit card payments. Please ensure that all personnel affected by these procedures are aware of these responsibilities on at least an annual basis. In the event a breach of this information or application of these processes is suspected, contact the Transaction Services and Finance Manager to ensure that the appropriate disclosure protocols are followed.