College Policy & Procedures Manual	
Category	Financial / Legal
Policy #	3.2.12

3.2.12 Credit Card Procedures

POLICY

The College will periodically obtain detailed credit card information from students or customers for the purposes of payment of outstanding balances to the College.

PURPOSE

The College of the Rockies currently accepts payment for its services via credit card. A majority of these transactions are processed via third-party payment processors, all of whom are compliant with the Payment Card Industry Data Security Standard (PCI DSS). However, a minority of credit card transactions are processed manually by College employees via credit card information provided by students or customers.

SCOPE

This policy applies to all situations where the College accepts payment where an employee manually processes a credit card transaction.

Transactions involving payments made by the College for goods and services, using either College credit cards or employees' personal credit cards, are excluded from this policy.

DEFINITIONS

Payment processor: A payment processor is a third party which processes credit card transactions and deposits funds into the College's bank account. At no point in the process does a College employee record or maintain information relating to the credit card. For example, as of the date of this policy, the College currently uses TD Merchant Services, PayPal and Global Payments as payment processors.

Cardholder, or credit card, information: Cardholder, or credit card, information refers to credit card number, expiry date, PIN number and card security code (the three digit number on the back of a credit card).

Manual transaction: A transaction where an employee manually enters credit card information provided by a student or customer, as opposed to automatically processing the payment by swiping a card, inserting a chip and PIN card, or having a student or customer enter card information directly into a payment processor.

Authored by: Controller *Approved by: CPC* *Current issue date: December 2017*
Scheduled revision date: December 2022

GUIDELINES

A. **Cardholder information storage - electronically**

A.1 No cardholder information should be stored by College of the Rockies in electronic form (email, Excel, Word, etc.).

A.2 Electronic files should be reviewed and any found containing cardholder information should be deleted.

B. **Cardholder information storage – hard copies**

The best practice is to destroy, shred or mask all hard copies containing cardholder information once the related transaction has been processed. If, for some reason, it is necessary to retain the cardholder information for a period of time:

B.1 Store all paper documents in a secure filing cabinet.

B.2 Restrict access to the filing cabinet on a business need-to-know basis.

B.3 Lock filing cabinet areas or offices when unattended and outside of business hours and secure key.

C. **Email policy**

C.1 College of the Rockies cannot control unsolicited emails from students or customers containing cardholder data; however, staff should not encourage students or customers to include cardholder information in emails.

C.2 Never email credit card information, either in the text of the email or in an attached document.

C.3 If an unsolicited email with credit card information is received, print the email and delete it immediately afterwards.

C.4 After the transaction is processed, destroy or shred the email hardcopy.

C.5 If, for some reasons, you need to retain other information provided on the email, follow the “mask credit card information” directions.

D. **Telephone policy**

If a student or customer would like to pay with a credit card over the telephone:

D.1 Take the credit card information on a blank piece of paper designed to collect credit card information. Do not use the back of another document.

D.2 Do not repeat the credit card information back to the student or customer unless you are isolated from the public; instead, have the student or customer repeat the information back to you for confirmation.

D.3 Secure the credit card information and process the related transaction within a short period of time.

D.4 After the transaction is processed, destroy or shred the paper copy containing the credit card information.

E. **Fax policy**

E.1 College of the Rockies staff should not encourage students or customers to include credit card information on faxes.

E.2 If a fax with credit card information is received, immediately secure the credit card information and process the related transaction within a short period of time.

E.3 After the transaction is processed, destroy or shred the fax.

E.4 If, for some reason, you need to retain other information provided on the fax, follow the "Mask credit card information" directions.

F. **Mask credit card information**

On any hard copies including credit card information:

F.1 Black out the first 12 digits of the credit card number and the Card Security Code. If you can still see the number when holding the document up to the light, perform the following:

- Make a copy of the blacked out document for our record keeping purposes.
- Destroy or shred the original hard copies.

G. **Data storage policy**

For credit card information that has been stored:

G.1 Review the stored information on an annual basis to determine if it is still necessary to keep.

G.2 Destroy or shred information that is no longer required for business reasons.