# Cash & Banking Procedures

# Clare College
# Cash & Banking Procedures

## Contents

# Clare College
# Cash & Banking Procedures

## 1. Banking Procedures

### 1.1 Receipt of cash and cheques within a department

All cheques must be made payable to Clare College.

It is the responsibility of the Head of Department to establish procedures which ensure that all cheques and cash received are given intact (i.e. no deductions) within one week, or more often if the sums received exceed £250, to the Bursary for banking.

The following are **not permitted** from any cash takings/receipts:

- The cashing of personal cheques even if the intention is to reimburse the float later
- The topping up of any petty cash float
- The payment of travel expenses or advances to employees
- The payment to individuals for services supplied (e.g. payments to visitors for travel expenses)
- The payment of external suppliers for services rendered

<u>Post dated cheques</u>

We should only accept post-dated cheques if it is unavoidable and only after referral to the Finance Manager.

### 1.2 Storage/security of cash and cheques within a department

All monies should be taken promptly to the Bursary as detailed in 1.1 and departments are responsible for ensuring cash and cheques are kept secure until they are handed over. Amounts up to £250 cheque/cash combination can be held in a locked drawer/cabinet in a secure office overnight. Amounts greater than this must be kept in a safe.

<u>Lost or missing cash</u>

In the event of cash being lost, missing or stolen, the Finance Manager must be notified immediately who will then inform the Bursar.

### 1.3 College bank accounts

The College currently has three bank accounts for paying in funds with Barclays:

- Bursar’s account
- Tutor’s account
- Development account

All College income, including donations, must be paid promptly into a College bank account and must be recorded in the College accounting system. Employees of the College have no authority to open bank accounts for the College.

### 1.4 Banking of sterling cash and cheques

All banking of cash and cheques is done through the Bursary. They will complete paying books, record the income on the accounting system and bank the cash and cheques into Barclays Bank.

### 1.5 Banking of foreign cheques

Wherever possible all transactions and receipts should be requested in pounds sterling. All foreign cheques will be taken to Barclays Bank for negotiation by the Bursary. Any bank charges and exchange rate differences will be a cost to the department.

## 2. Debit and Credit Card Receipts

### 2.1 Introduction

An efficient method of receiving payments is to accept debit or credit cards. This section covers the procedures and legal requirements the College must adhere to.

### 2.2 Accepting card payments

There are two different ways to accept card payments. Transactions can be accepted where:

a. the card holder is present; or
b. the details of the card are entered manually (card holder not present).

‘Card-present’ and ‘Card-not-present’ refers to whether the customer has presented the card for processing in person and is required to either enter their chip-and-pin number or sign a form.

We accept all major cards such as Visa, MasterCard, Maestro and Solo.

Under no circumstances must card details be accepted by either email or via a networked fax.

**Surcharges for paying by card**
At each terminal there will be a notice displayed (under Payment Services Regulations 2009) clearly stating surcharges to be made as follows:

| **Card Type** | **Surcharge** |
|---|---|
| Debit cards | Free |
| Credit cards<br>transaction value up to £100 | Set fee of £3.00 per transaction |
| Credit cards<br>transaction value over £100.01 | 3% of amount of each transaction |

If the card holder is not present then these surcharges must be communicated and accepted before processing the payment.

## 2.3 PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The standard was created to help prevent payment card fraud through increased controls around the data and its exposure to compromise and applies to all organisations that hold, process or exchange cardholder information.

It is our responsibility to ensure card details and personal data on customers are stored securely by us (and any third party which stores, transmits or processes such card data on our behalf) and only used for the purposes intended. The cardholder must be able to feel confident the College is taking all necessary measures to safeguard their personal details.

Card details must never be transmitted through email as this is considered an unsecure environment.

The College must meet these PCI DSS standards at all times to remain a member of the card scheme and to ensure that we can continue to have the ability to process card payments. An annual audit is carried out based on our Merchant Level which is dependent on the number of card transactions processed per year.

### 2.3.1 The PCI DSS Standards

The standards are detailed in full on the PCI website at https://www.pcisecuritystandards.org/ but thy can be summarised into the following 12 requirements:

| | | |
|---|---|---|
| Build and Maintain a secure Network | 1 | Install and maintain a firewall configuration to protect cardholder data. |
| | 2 | Do not use vendor-supplied defaults for system passwords and other security parameters. |
| Protect Cardholder Data | 3 | Protect stored cardholder data. |
| | 4 | Encrypt transmission of cardholder data across open, public networks. |
| Maintain a Vulnerability Management Program | 5 | Use and regularly update anti-virus software or programs. |
| | 6 | Develop and maintain secure systems and applications. |
| Implement Strong Access Control Measures | 7 | Restrict access to cardholder data by business need to know. |
| | 8 | Assign a unique ID to each person with computing access. |
| | 9 | Restrict physical access to cardholder data. |
| Regularly Monitor and Test Networks | 10 | Track and monitor all access to network resources and cardholder data. |
| | 11 | Regularly test security systems and processes. |
| | 12 | Maintain a policy that addresses information security for all personnel. |

### 2.3.2 The College Policy

The Bursar is responsible for ensuring the College is PCI DSS compliant and its policy includes the following:

- The College will undertake a PCI Compliance review on an annual basis.
- If anyone identifies that this policy is compromised or is at risk of compromise this must be reported to the Bursar immediately.
- All staff who handle either customer present or customer not present card transactions in any form must undertake PCI Compliance training on an annual basis.
- All customer present card transactions must take place using a PCI compliant electronic point of sale system.
- Customer not present card transactions should be limited and other payment methods used if available.
- Card and/or cardholder details must not be stored or transmitted electronically (other than through the Colleges on-line facilities). This includes emailing and scanning of paper copies.

- If there is a valid requirement to scan documents that also contain card transaction details, the card details must be obliterated using an indelible marker pen before scanning.
- Where possible, any paper notes/or paper copies containing card transaction details must be destroyed (cross shredded) immediately after use.
- Where paper copies containing card transaction details need to be retained for a valid reason i.e. chargebacks, they must be retained in a secure, locked cabinet or room at all times.
- The retention period for all paper copies containing card transaction details is :
  - Merchant copies should be kept for a minimum of 6 months (this is the time limit with which chargebacks can be registered).
  - Beyond this, copies should be kept for a further 12 months

  **(i.e. TOTAL storage time equals 18 months for the date of transaction)**

  - File by date of transaction.

## 2.4 PDQ Terminals

PDQ (Process Data Quickly) terminals enable credit or debit cards to be used in a swipe card reader that is Chip and PIN (Personal Identification Number) enabled. It is a secure method of taking payments when the customer is present. The terminals may also be used for taking card payments when the customer is not present.

### 2.4.1 Taking payments when the customer is not present

Customers should be told not to send their card details by e-mail instead they may give the information over the phone, by fax or by post. Care must be taken to ensure that these details are kept secure at all times.

The person authorised to use the PDQ terminal manually enters the necessary customer and card details. It is imperative the department takes upmost care to ensure the transactions receive Authorisation and the customer card data matches.

### 2.4.2 Daily task for the department

At the end of each working day which included a PDQ terminal transaction, the department must take a Z-reading to ‘clear’ the terminal and give a daily transaction total. This till slip must be attached to the relevant sales slips from the day and passed to the Bursary on the following day.

### 2.4.3 Storage of the terminal and supervisor card

During normal working hours, the terminal should not be left unattended unless it is in a secured environment (i.e. locked office).

Both the PDQ terminal and the supervisor card must be stored in a secure manner in which unauthorised persons cannot access it out of working hours. It must not be switched off as Barclaycard may need to send notifications and updates during the evening.

### 2.5 Refunds

There will be occasions when it Is necessary to refund a payment charged to a customer's card is necessary e.g. cancellation of a conference booking.

Refunds must be made in the same manner as the original payment e.g. customer cannot be refunded by cash or cheque if the original payment was made by credit or debit card. The same card should be used for the refund.

If the card holder is present, follow the instructions provided in the Terminal's User Guide which will include the customer entering their PIN to verify the transaction.

If the card holder is not present, follow the instructions provided in the User Guide and ensure the customer receives the customer-copy of the refund receipt.

If the original payment card has expired/been stopped then please contact the card holder.

### 2.6 Chargebacks

A chargeback is the return of funds to a customer which is forcibly initiated by the customer's card provider. Card customers have a right to make a chargeback against the payment up to six months from the original transaction date. Chargebacks may occur when the card holder does not recognise a transaction on their bill (i.e. in the case of identity fraud or clerical error) or if they claim that they have never received the goods or service. The customer will query the transaction with their card provider who will credit their bill with the value if the vendor is not able to prove the sale was valid.

When chargebacks are made against the College, Barclaycard will contact the Bursary with some details of the transaction. They will provide the original date, the value and some of the card number. They will NOT provide the name of the card holder – therefore, PDQ receipt must not be filed by the customer's name (see 2.8).

The Bursary will trace the transaction and contact the relevant department for further details on the transaction. The College will have 10 days to reply to Barclaycard with the necessary documentation to prove the transaction was valid.

### 2.7 Document Retention

The security of card and customer data is mandatory to ensure the College is PCI DSS compliant.

### 2.7.1 What information must NOT be stored at any time?

- The contents of the magnetic stripe also known as Track 2 Data.
- The Card Verification Value or CVV contained in the magnetic stripe.
- The Card Verification Value contained in the magnetic stipre image in the chip known as the iCVV.
- The Card Security Code also known as CVV2 printed on the back on the card in or next to the signature pane.
- The PIN Verification Value or PVV which is contained in the magnetic stripe.
- Passwords or pass phrases.

### 2.7.2 What information must be stored securely?

Any information that is used to authenticate a card payment including but not limited to:

- the card number
- expiry date
- issue number
- any other unique data supplied as part of the card payment

Any information that could identify individual card holders and their purchases including:

- name
- address
- purchase description
- amount
- other details of the card payment

### 2.7.3 Physical Storage

Where paper copies containing card transaction details need to be retained for a valid reason i.e. chargebacks, they must be retained in a secure, locked cabinet or room at all times.

Store documents in original transaction date or card number order. If there is a query relating to a transaction, Barclaycard will not provide the customer’s name. Copy credit card receipts must not be sent back to the customer unless part of the credit card is obscured.

### 2.7.4 Electronic storage – NO!

Card and/or cardholder details **should not** be stored or transmitted electronically. This includes emailing and scanning of paper copies.

If there is a valid business requirement to scan paper copies of documents which also contain card transaction details, the card details must be obliterated using an indelible marker pen before scanning. Where possible, any paper copies containing card transaction details must be destroyed (cross shredded) immediately after use.

### 2.7.5 Period of retention

Merchant copies of transactions must be retained in a secure and accessible place for minimum period of 6 months. Customers can action a chargeback against a transaction during this time. For internal audit purposes, transaction details should be retained for a further minimum period of 12 months.

**i.e. TOTAL storage time is 18 months from the date of the transaction**

*Note, if you have made a rough paper note of any card details prior to entering them into a PDQ machine or on a template form these should be securely destroyed once details have been transferred.*

## 2.8 Preventing Fraud

We all have a part to play in the prevention of card fraud so always be vigilant.

When the cardholder is present and the card is issued with a title, ensure the customer matches the title (e.g. ‘Mr.’ is printed on the card, and the customer is male). If you suspect there is an attempted fraud, contact the Finance Manager with full details of the transaction and for advice on what steps need to be taken.

## 2.9 Staff Training and Recording

It is important that all staff involved with the accepting of card data either when the customer is present with their card or not is aware of these procedures outlined in this chapter and the PCI Standards. This includes all shift, seasonal, permanent and temporary workers.

The Department should maintain a list of all those currently authorised to use PDQ terminals.

All staff should on an annual basis complete ‘refresher training’ to remind themselves of the standards and protocols that must be adhered to. In addition any new staff should receive training on the requirements as part of their induction.

## 3. Petty Cash

### 3.1 Purpose of petty cash

This procedure aims to ensure:

- There is an accurate account of all petty cash expenditure
- Control is maintained over both the nature and level of expenditure
- Security measures are in place to minimise the potential for fraud/misuse of petty cash

The College Bursary holds petty cash which is available to all Departments under the conditions for using petty cash as detailed below in section 2.2.

Some Departments may request to hold a petty cash float (normally up to a maximum of £100) – see section 2.3.

### 3.2 Conditions for using petty cash

- Petty cash must be used exclusively for expenditure directly relating to College business. Under no circumstances must petty cash be used to make payments to external suppliers for services rendered.
- Petty cash must **not** be used to reimburse mileage or other travel costs. In these cases College Expense forms should be used.
- Petty cash must **not** be used for personal expenditure even if the intention is to reimburse the float later.
- Payments from petty cash shall be limited to items of expenditure below the cost of **£25**.
- All payments from petty cash **must** be supported by a receipted voucher.
- Expenditure claimed should always be authorised by someone other than the claimant (Head of Department or College Officer).
- Claimants receiving reimbursement must sign for receipt of monies.
- Staff responsible for the petty cash float must ensure the records are always up to date.
- Petty cash floats will not be replenished until all coding information is up to date
- There must be monthly independent checks of petty cash balances and use.
- Heads of Department are responsible for the security of any float and for ensuring that all expenditure is properly supported and authorised.
- Departments are required to certify their petty cash float at the end of the financial year.

## 3.3 Department request for a petty cash float

- Requests for a petty cash float and any permanent, or temporary, increase to an existing float must be made in writing by the Head of Department to the Finance Manager clearly stating the amount of petty cash float required (this is normally a maximum of £100).
- The Finance Manager will review the request and if approved inform the Head of Department to collect the float from the Bursary
- The Bursary will maintain a list of each department's petty cash limit.

## 3.4 Petty cash imprest system

Each department will need to establish a Petty Cash Imprest System for recording all petty cash received in and paid out.

A summary of the details for each petty cash transaction completed should be transferred to the Imprest Form (Appendix A), which is used for replenishing the petty cash float and as a basis for the Bursary to prepare a journal to post the transactions on to the accounting system.

## 3.5 Reconciling the imprest system

As part of the department's month end procedures the petty cash imprest system balance must be reconciled to the actual cash in hand and signed off by the Head of Department.

## 3.6 Replenishing the petty cash float

A copy of the completed imprest form and all accompanying receipts should be passed to the Bursary within the first week of the following month. They will check this form and replenish the float up to the agreed limit. The Bursary will refuse to replenish floats if discrepancies with the imprest form are found, pending approval from the Finance Manager.

In cases where there has been no activity for a period of three months or more, then the department, together with the Finance Manager, should re-assess the need for and the level of a float.

## PETTY CASH IMPREST FORM

DEPARTMENT_______________________________________

| Date | Cost Code | Amount | Description |
|---|---|---|---|

TOTAL ________________

CASH IN HAND ________________ Balance of cash in hand checked & found correct

TOTAL IMPREST ________________

Signed_______________________________________(Head of Dept)