RECEIPTING AND BANKING PROCEDURES 2018

Issued by:	Chief Financial Officer
Dated:	25 October 2018
Last amended:	25 October 2018
Signature:	
Name:	Wayne Andrews

---

1 Purpose and application

(1) These procedures apply to:

(a) the collection, receipting, recording and banking of all revenue paid to the University; and

(b) all staff and affiliates.

2 Commencement

These procedures commence on 25 October 2018.

3 Interpretation

banking agent	means a staff member of a University organisational unit authorised by the Order to Cash Manager, Financial Control and Treasury (FCT) to deposit revenue from external sources into the University's bank account.
cardholder information	means the data found on the front and back of a credit or debit payment card, which includes: • Primary Account Number: the card number which can be up to 16 digits; • Cardholder's name; • Expiration date (month/year); and • Security number or CCV: a 3 or 4 digit number on the back of the card.
EFTPOS	means electronic funds transfer point of sale.
FCT	means the Financial Control and Treasury unit in the University's Finance professional services unit.

merchant	means the holder of a banking facility that enables the holder to accept payments by debit payment card, credit payment card or EFTPOS.
PayOnline	means the University's cashiering system used to record revenue transactions and refunds.
PCIDSS	means the Payment Card Industry Data Security Standard, determined by Australian Payment Card Industry Security Standards Council.
receipting	means acknowledging a payment has been received using the PeopleSoft Financials system.
trade debtor payments	means accounts receivable trade debtor invoice payments.

4 General principles

(1) Everyone involved in collecting, receipting or holding University money must do so consistently with the principles stated in this clause.

(2) **Safeguard University money,** including:

(a) minimising the potential for significant amounts of cash being retained on University premises overnight; and

(b) using a suitable safe or locked cash box for the retention of cash.

(3) **Be aware of and manage work health and safety risks with cash handling.** In the rare occurrence of handling cash, staff can refer to Safe Work Australia Guide for handling and transporting cash.

Note: Campus Security can provide assistance in arranging a security firm to provide cash-in-transit services.

(4) **Protect cardholder information and meet the security standards under the PCIDSS.**

(a) The University is a merchant under PCIDSS and must protect cardholder information against fraud.

(b) The 12 PCIDSS standards that the University must comply with are specified in Schedule 1.

Note: Refer to the finance staff intranet information on Payment Card Industry Data Security Standards.

(c) Everyone accessing cardholder information must:

(i) not store cardholder data outside the approved University systems.

Note: Storage includes paper, photocopy, spreadsheet, scan and email.

(ii) avoid sending or receiving card information by email;

(iii) not use the vendor's supplied defaults for passwords;

(iv) not store system IDs and passwords on computers or papers near computers;

(v) not share system IDs and passwords with colleagues; and

(vi) maintain up-to-date antivirus software.

(5) **Do not mix private funds with University funds**, including:

(a) not cashing a personal cheque from University funds; and

(b) not banking any private money in a University bank account.

5 Receiving and banking revenue

(1) The University receives revenue from a variety of sources, including students, commonwealth and state governments, industry and private donors.

(2) Details of the following are available from the finance staff intranet:

(a) the main revenue types;

(b) the organisational unit that issues payment invoices;

(c) the organisational unit that receives and banks the revenue; and

(d) the organisational unit that manages and reconciles the revenue.

(3) Receiving and banking University revenue is managed by banking agents, using either of PayOnline or manual receipting.

(a) Revenue received by a banking agent must be deposited daily into a University bank account.

(b) If the daily revenue received is less than $500 then it must be banked within five working days of collection.

(4) **PayOnline**

(a) Payments to the University can be made by debit or credit card, BPay and Western Union.

(b) Refunds are managed by the Cashier after authorisation from a delegated officer. A Deposit/receipt: Credit Card Refund Request form must be completed and sent to the Cashier for processing.

(c) PayOnline integrates overnight with the University's general ledger financial system.

Note: The PayOnline Administrator manages access to the PayOnline system via a Pay Online Request (select ICT services then Finance and then the Pay Online Request form).

(5) **Manual receipting by banking agents:**

(a) Direct Deposit forms must be completed on the day of banking by the banking agent and returned to the Cashier to reconcile with the bank deposit amounts.

(6) **Manual receipting by non-banking agents**:

(a) Any person who is not, or does not work in, a banking agent must:

(i) complete a Deposit/receipt: Cashiers Office form for any payments received; and

(ii) take or send the form and the payment to the Cashier for banking.

Note: The Cashier, FCT does not accept cash payments.

(7) **Bequests and Donations:**

(a) Advancement Services manages all revenue received for bequests, donations, and grants by non-government organisations.

(b) Any person who receives payments for bequests or donations must:

(i) complete a Deposit/receipt: Advancement Services form; and

(ii) take or send it and the payment to Advancement Services for banking.

(8) **Trade Debtor payments**:

(a) The Cashier manages all revenue received for trade debtor payments, unless a banking agent has been authorised by the Order to Cash Manager, FCT to bank trade debtor payments.

(9) **Receiving foreign currency revenue**:

(a) Any person receiving foreign currency revenue must:

(i) complete a Deposit/receipt: Cashiers Office form; and

(ii) take or send it and the payment to the Cashier for banking.

(10) **Unidentified revenue**:

(a) All unidentified and surplus revenue received should be banked immediately and credited to a suspense account.

(b) The Cashier is responsible for clearing unidentified payments in the suspense account and liaising with the banking agent to identify the revenue.

(11) **GST**:

(a) GST will be calculated in the finance systems depending on the GST status code assigned to the revenue by the banking agent.

(b) The finance systems show revenue net of GST for the relevant organisational unit.

6 Issuing a receipt

(1) A banking agent may issue a receipt on the request of the payer.

(2) Receipts should be issued electronically and emailed to the payer.

(3) Any manual receipts issued must be:

(a) produced on an official University receipt book;

(b) typed or written in ink; and

(c) signed by a banking agent or other authorised staff member.

(4) Any duplicate receipts issued must indicate they are a duplicate or reprint.

(5) The receipt number must be written on the back of any payment documentation for reference purposes.

7 Cancelling a receipt

(1) A reason for the cancellation must be written on the back of the printed receipt or documentation and stored with documentation for the day's banking.

8 Bank rejected card payments and dishonoured cheques

(1) The Bank Reconciliation Officer, FCT will receive information from the bank that a cheque or merchant card transaction has been rejected and will inform the Cashier.

(2) The Cashier will cancel the rejected receipt in the University finance system, indicating that it was dishonoured by the bank, and notify the relevant banking agent.

(a) For rejected domestic student fees and trade debtor payments, Order to Cash, FCT will contact the payer requesting a new payment.

(b) For rejected international student fees, International Office will contact the student requesting a new payment.

(c) For all other rejected payments, the relevant organisational unit will contact the payee requesting a new payment.

9 Rescissions and replacements

This document replaces the Receipting and Banking Procedures, which commenced on 13 December 2011, which is rescinded as from the date of commencement of this document.

NOTES

Receipting and Banking Procedures 2018

Date adopted: 25 October 2018

Date commenced: 25 October 2018

Administrator: Director, Financial Control and Treasury

Review date: 25 October 2023

Rescinded documents: Receipting and Banking Procedures

Related documents:

AMENDMENT HISTORY

Provision	Amendment	Commencing

Schedule 1: PCIDSS Standards

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 data.
	4. Encrypt transmission of cardholder data and sensitive information across public networks.
Maintain a vulnerability management program	5. Use and regularly update anti-virus software.
	6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to data by business need-to-know.
	8. Assign a unique ID to each person with computer 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.
Maintain an information security policy	12. Maintain a policy that addresses information security.