

# Flemington Primary School

## Electronic Funds Management Policy



### 1. PURPOSE AND RATIONALE:

Electronic (internet) banking offers an online facility (via a website) which provides users with the ability to undertake various banking functions, such as checking account balances, transferring funds between accounts, direct debit, direct deposit, BPAY payment/ receipts and EFTPOS (Electronic Funds Transfer Point of Sale).

In order to minimise risks, guidelines are to be adhered to, in accordance with the 'School Electronic Funds Management Policy and Guidelines' (January 2015) as issued by the Department of Education.

### 2. POLICY STATEMENT:

Key points are as following:

#### **Financial Management**

The School's Principal and Business Manager must ensure that the official account is not overdrawn. Therefore, an understanding of the school's cash flow position and commitments due, are critical to the use of electronic funds for the payment of invoices and receipting funds.

#### **Internal Controls**

- Delegations – as approved by school council;
- Security and confidentiality of passwords and data at all times;
- Documentation kept by the school confirming all transactions related to the account(s) such as purchase orders, tax invoices, payment vouchers, payroll listings, relevant CASES21 reports;
- Appropriate segregation of duties to ensure and maintain the accuracy and legitimacy of accounts and transactions. This can be implemented, by alternating sequential tasks, so that no one person has complete responsibility for the entire transaction, provided that some separation occurs between key activities. Functions that should be separated include authorisation, payment, custody and recording.

#### **School Records Management and Archives**

Records documenting the management of banking activities, including deposit records, bank statements, bank reconciliation statements, investment and dividend statements, and records documenting the use of credit cards to be kept for 7 years after the completion of the financial year in which the record was created.

This Policy is based on the DEECD Finance and Accountability Policies and the Finance Manual.

### 3. DEFINITIONS:

- None.

### 4. ACTION GUIDELINES:

#### 4.1 Electronic Payment of Accounts

Electronic payments can be made from the official account via the following methods:

- Payments to creditors via direct debit account credit
- BPAY;
- Direct Deposit; and
- Local payroll processing.

Payments through internet banking software are effectively just another form of payment and must still be authorised by two authorised officers. A single authoriser of payments via internet banking software is a clear breach of the regulations governing the payment of accounts by schools.

The school business manager cannot be nominated as an authoriser under this regulation even if he or she is a member of the school council.

#### **Direct Debit Payments**

The direct debit facility effectively allows an external source e.g. financial institution, supplier etc. to remove or 'sweep' funds pertaining to a pre-arranged amount and date from the school's official bank account on a regular or ad hoc basis e.g. computer lease payment.

- How to use Direct Debit

The school should ensure that it receives a tax invoice/statement from each supplier prior to the direct debit 'sweep' date each month in order to confirm the accuracy of all payment's as well as any cash flow considerations. If the direct debit differs in amount or timing, the supplier must be contacted immediately and the issue resolved or the direct debit cancelled.

#### **BPAY Payments**

BPAY differs to direct debit in that the school has full control of the payment with regards to the payment date and amount of the expenditure. BPAY is essentially an alternative to payment by cheque and employs the use of electronic (internet), telephone or 'pay in person' for transfer of funds from the school's official account to the supplier. Schools must ensure that suppliers'/creditors' accounts are always paid by the due date and for the correct amount.

BPAY is a secure electronic banking product identified on a supplier/creditor account with a unique biller code. The payee selects either the internet or telephone option to transfer funds from the school's official account to the supplier and follows a series of steps to attach the amount owed to the creditor's account and biller code.

With BPAY transactions the standard controls related to creating an order, setting up the commitment and determining the date and amount for the transfer can be easily maintained by schools.

- How to use BPAY

Schools will receive an invoice in the normal manner. The invoice should then be attached to the pre-approved purchase order and forwarded to the principal for approval for payment.

Once payment has been made using BPAY, the BPAY receipt number and details of the transaction should be printed from the internet banking website. This printed receipt should then be attached to the original payment approval/invoice.

### **Direct Deposit**

Direct Deposit via an internet banking facility provides schools with the freedom and flexibility to pay creditors (creditor, school level payroll employee) by nominating their BSB and account number at the time of the transaction.

A business banking package that has a two user authorisation of payments (such as Commonwealth Banks "CommBiz") is recommended as it contains a greater degree of security and access controls.

- How to use Direct Deposit
  - Complete all processes for the payment on CASES21.
- Creditors
  - Entry of purchase orders; and
  - Entry of invoices
- School Level Payroll
  - Processing of payroll;
  - Generation of payment;
  - Printing and signing of payment vouchers;
  - All transactions are authorised by the appropriate delegate;
  - Reconcile the payments to CASES21 reports; and
  - Retain appropriate documentation.

## **4.2 Electronic Revenue**

School is able to accept alternative methods to cash or cheque receipts into the official account via the following methods:

- EFTPOS
- BPAY
- Third party internet revenue collection

### **Internal controls**

The principal will be responsible for ensuring that staff operating the merchant facility, are made fully aware of security requirements, and that all data obtained through processing EFTPOS transactions remains safe from fraud. Staff authorised to process transactions should be minuted at school council and entered into a register.

The internal controls in relation to EFTPOS include:

- Appointment by school council of an authorising officer for approval of phone and refund transactions (principal and/or their delegate).
- Physical security of EFTPOS machines.
- The number of terminals that will be installed and their locations and refund limits
- Documentation kept by the school confirming all transactions such as merchant copies of EFTPOS receipts, void receipts, refunds, daily EFTPOS reconciliation reports, authorisation details, relevant CASES21 reports.
- The appropriate segregation of duties to ensure and maintain the security, accuracy and legitimacy of transactions. This can be implemented, by alternating sequential tasks, so that no one person has complete responsibility for the entire transaction, provided that some separation occurs between key activities. Functions that should be separated include authorisation, payment, custody and recording.
- Establishment of an EFTPOS user register outlining the name of the school user, their unique ID (if one exists) and the EFTPOS functions they are authorised to perform.
- Staff familiarisation with the EFTPOS facility's functionality and User Guide provided by Financial Institution.
- Register of void or refund transactions.
- Procedures and documentation for processing phone and offline receipts and refund transactions
- Procedures for the use of mobile terminals around the school.
- Setting of minimum and maximum refund transaction limits.
- Reconciliation of monthly EFTPOS statement received from the school's financial institution with CASES21 transaction records.
- Reconciliation of daily EFTPOS settlement statements with CASES21 transactions.

NOTE: School must not have the 'Cash Out' configuration activated.

School EFTPOS terminals should be connected to the bank via phone connection and not via the internet. Connection via a phone line ensures that schools are not collecting or storing customer data in a manner that makes them susceptible to fraudulent transactions.

Passwords must be securely stored in line with the Departments ICT Security Policy. Any documentation must not include passwords. If passwords are recorded, they shall be maintained in a separate document and stored in a fire proof safe.

#### **Phone/Mail EFTPOS transactions**

- Only transactions on credit cards can be accepted via telephone or post; transactions on debit cards require the cardholder to be present at the point of sale.
- The School must ensure the information collected in order to undertake EFTPOS transactions must only be used for the specified invoice.
- The name of the cardholder should be the same as the name on the invoice. If the names are different a query should be raised with the debtor as to the reason for the difference. Once satisfied that the transaction is valid the principal or authorised officer should sign the form to approve the transaction including verification of the identification.

- Full card details including card number, expiry date and security code (when required) should be obtained and confirmed by discretely reading them back to the customer and the transaction should be processed while customer is on the phone.
- Both the EFTPOS and CASES21 receipt must be forwarded to the cardholder as their record of the transaction.
- When processing a credit card transaction that requires a signature for authorisation, schools should ensure that the signature obtained on the merchant receipt matches the signature on the card and that the signature panel has not been altered in any way.
- When processing a credit card transaction that requires the entry of a PIN, customers should be able to enter their PIN without risk of disclosure, and the PIN should never be recorded by the school.
- The School should ensure that the card number that is embossed on the card is free from alteration and that the card has not expired.
- Receipts should be entered onto CASES21 at the time the EFTPOS transaction is processed and both original receipts (EFTPOS and CASES21) issued. In circumstances where this is not possible, a manual school receipt can be issued at the time, with the CASES21 receipt forwarded when it is entered on to the system. An authorised officer should reconcile all manual receipts to CASES21 to ensure all funds received by the school are receipted.
- The School should always print both the merchant and customer copies of the receipt for both credit and debit card transactions, and retain the merchant copy for audit purposes.

#### **Incorrect transaction processing**

Void transactions must be processed on the same day as the original transaction. After that period it must be treated as a refund as per the procedures under 'Refunds' included in these guidelines.

- All documentation relating to the original transaction must be obtained
- The void transaction must be signed by the cardholder
- Copies of both the original and voided transactions should be retained for audit purposes
- The school copy should be signed by the authorised officer and where possible this should not be the operator who processed the original receipt. The transaction details should be recorded in an EFTPOS 'void transaction' register.

#### **Refunds**

If an EFTPOS refund transaction has been processed and the receipt entered on CASES21, the following refund guidelines should be applied:

- Before a school processes a refund, the original receipt is to be produced or the receipt number identified.
- The refund request pro-forma must be approved by an authorised officer (e.g. principal) prior to processing. This will ensure segregation of the authorisation of refunds from the processing of the refund.

- The School should develop a refund request pro-forma to be completed each time an EFTPOS refund is requested. It should include:
  - name of cardholder,
  - card number,
  - transaction details,
  - date,
  - name of staff member processing transaction, and
  - signature of cardholder and principal.
- The document should be filed securely with limited access
- Refunds can only be made to the account of the cardholder that made the original payment.
- EFTPOS transaction refunds must not be made by cash.
- If the refund is not performed on the same day as the receipt, the school should not process the refund until they have confirmed the funds have been credited to their official account by the settling bank.
- Refund can be made by cheque following normal processes, or via the EFTPOS terminal to the cardholders account (principal authorisation is required for both instances).
- Cardholders should be notified that it could be 2-3 business days before the refund may reach their account.
- The cardholder should be given the customer copy of the refund voucher and must sign the merchant copy which is to be retained by the school.
- The EFTPOS refund should be processed on the terminal and CASES21 on the same day. The original receipt and merchant copy of the refund is to be attached to the CASES21 payment voucher which must be checked and approved by the authorised account signatories before being processed on the EFTPOS terminal
- The refund should be recorded in the EFTPOS void or refund register.

### **Banking**

- Schools use a separate receipt batch (not containing cash or cheque transactions) for EFTPOS receipts which is updated at the end of each day
- The Settlement\* on the terminal is also performed at the same time as the batch is updated. The daily total on each should match (unless adjustment is required due to processing of a refund)
- On the Bank Reconciliation, the batch total for that date (less any refunds) should match the direct credit amount paid by the bank.

*\* The Settlement process is where the days EFTPOS transactions are closed off for the day and a total is determined. If the Settlement is not performed by the school each day, the bank will "force Settlement" at a time determined by them. As a result, one or more Settlements may cross over one or more batches containing EFTPOS transactions making it difficult for schools to reconcile the EFTPOS transactions on their Bank Reconciliation.*

- The School should to perform settlement each day at a time determined by the school.

## **BPAY Receipts**

BPAY is an electronic bill payment service providing families with the option of paying their school account at any time, day or night, on any day of the year via telephone or internet banking.

BPAY receipting for families has been introduced into CASES21 Finance and will allow schools to provide BPAY facilities to their families.

Setting up of BPAY in CASES21

- By default, BPAY receipting will not be enabled in CASES21. Schools wishing to use the functionality will need to activate BPAY receipting.

## **5. MONITORING, REPORTING AND REVIEW:**

**Direct Debit** information to be retained by School

- All details provided by the supplier relating to the amount, date of direct debit and regularity of the payment;
- Original payment approval usually via an application for direct debit form (signed by principal and a designated signatory of school council);
- Schedule and timing of deductions (if not included in the above);
- All related billing and statement details; and
- Relevant CASES21 Finance reports.

**BPAY Information** to be retained by the School

- Original signed payment approval and creditor invoice;
- Printout of BPAY receipt (if processed through the internet), clearly displaying BPAY receipt;
- Reference number and date of transaction;
- If the phone is used to action a BPAY payment, the BPAY receipt number and date of transaction should be noted on the original payment approval/invoice information;
- The Principal should verify that the details on the tax invoice are identical to the screen print, particularly the biller code and BPAY reference number; and
- Relevant CASES21 Finance reports.

**Direct Deposit** information to be retained by the school

- The school council minutes that record prior approval utilisation of the direct deposit basis of internet banking;
- The school's approved Schools Electronic Funds Management Policy document;
- The safe and secure storage of all documentation;
- The provision of printed documentation to finance committee, school council and school auditors; and
- Relevant CASES21 Finance reports.

**EFTPOS** information to be retained by the school

- Minutes of school council meeting approving the use of the facility;
- EFTPOS policy approved by school council;
- Register of approved school users;
- Register of voided/refunded transactions;
- Pro-forma/documents containing transaction details;
- Merchant copies of EFTPOS terminal receipts, voided/cancelled receipts and settlement documents;
- Applicable CASES21 reports; and
- Daily EFTPOS reconciliation reports and documentation in support of refunds and/or adjustments.

## **6. RELATED POLICIES AND DOCUMENTS:**

- Cash Handling Policy
- Investment Policy
- Parent Payment Policy

## **7. REFERENCES:**

- DET School Electronic Funds Management Policy and Guidelines  
<http://www.education.vic.gov.au/Documents/school/principals/finance/guideelectronicfunds.pdf>
- DET School Financial Guidelines  
<http://www.education.vic.gov.au/school/teachers/management/finance/Pages/guidelines.aspx>
- DET ICT Security  
<http://www.education.vic.gov.au/school/principals/spag/infrastructure/Pages/ictsecurity.aspx>

## **8. REVISION HISTORY:**

This policy was ratified by School Council on July 30<sup>th</sup>, 2018.

This policy will be reviewed as part of the school's annual review cycle and be approved by School Council.