State Government Victoria

Department of Education and Early Childhood Development

Schools Electronic Funds Management Guidelines

A guide to electronic payments and receipts

Published by the Financial Services Division
Department of Education and
Early Childhood Development
Melbourne
July 2010

Authorised by the Department of Education
and Early Childhood Development,
2 Treasury Place, East Melbourne, Victoria, 3002.
ISBN [to be inserted if required]
This document is also available on the internet at
[http://www.education.vic.gov.au/management/financial/policy.html].

Contents

1. Introduction

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, schools should be reminded of the compliance requirements in the ***Education Training and Reform Regulations 2007***, section 37(1) Revenue and Expenditure which outlines that all cheques and **negotiable instruments** drawn on any account kept under the control of a school council **must be authorised by the principal and a member of the school council nominated by the school council** for that purpose.

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.

A single authoriser of payments via internet banking software is a clear breach of the regulations governing the payment of accounts by schools.

Schools should develop and gain endorsement of a Schools Electronic Funds Management policy that outlines decisions made by School Council regarding the schools use of electronic funds, the scope of the implementation, internal controls required to be implemented, permissions and delegations, retention and storage of documentation etc.

Financial Management

Principals and Business Managers 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.

Prior to utilising any form of internet banking software, the school council needs to give consideration to:

- the associated costs and benefits for the school of using the software
- fraud prevention
- information privacy
- internal control implications.

All decisions and modifications to prior decisions made by school council in regards to internet banking must be minuted and tabled for approval at school council.

Internal Controls

Internal controls to support the use of electronic funds will minimise the potential financial risk to the school and its available funds. The various internal controls that need to be considered include:

- delegations – school council should review the current list of staff with authority to approve purchase orders, pay invoices, receive funds and extend this review to electronic procedures, including the upper dollar limit.
- IT Security - access levels to proprietary applications should be in line with approved delegations. All changes to financial delegations should be included in school council minutes and filed appropriately as a permanent record
- proper authorisation and approval of both the initial setting up of account details and any subsequent transactions against the account(s)
- completeness and accuracy of all details so they can be verified by a responsible officer
- 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
- the 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 council reporting and monitoring
- bank imposed security issues.

To assist in the preparation and development of appropriate school internet banking procedures and practices, consideration of the following information available on the Financial Management Website is critical:

- Internal Control for Schools
- School Finance Manual

Payments through internet banking software are effectively just another form of payment and as such, any payments must still be authorised by two people.

Privacy

The use of electronic payments and receipts will require schools to acquire and retain customer information. Schools must do so in accordance with *Schedule 1 of the Victorian Information Privacy Act 2000*.

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 have a **temporary** disposal action status as per 5.1.3 of the PROS 07/01 General Retention & Disposal Authority for Records of Common Administrative Functions: destroy 7 years after the completion of the financial year in which the record was created.

Guidelines are issued by the Public Records Office to provide a mechanism for the retention and disposal management of school records in accordance with the Public Records Act 1973. Schools providing electronic payments and receipts need to maintain these guidelines.

For information regarding records please refer to the following documents available on the Public Records Office Victoria website:

- PROS 01/01 General Disposal Schedule for School Records
- PROS 07/01 General Retention & Disposal Authority for Records of Common Administrative Functions

Further information is available at Archives and Records Management Advice for Schools.

Storage and Disposal

The secure storage and disposal of records documenting the use of credit cards to meet the requirements of both the Victorian Information Privacy Act 2000 and the Public Records Act 1973 should be a high consideration for schools.

To assist, schools should consider implementing the following suggestions for the secure storage of paper and computer records of credit card and EFTPOS details:

- Credit card numbers blacked out with the exception of the last four digits (eg **** **** **** 1234)
- Documentation filed in a secure location with restricted access

Records may only be destroyed in line with the Public Records Office guidelines, by approved methods of destruction. Approved methods of destruction are:

- deletion of electronic records,
- shredding,
- pulping,
- burning,
- chemical recycling (for microform/x-rays), and
- dissolving in acid.

Burying or dumping records are **not** approved methods of destruction.

2. Electronic Payment of Accounts

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

- Direct Debit
- BPAY
- Direct Deposit

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.

An important feature of dedicated internet banking software, and in particular the ability to process creditor/payroll and related payments through direct debit and BPAY, is that the payment is directed to one creditor/payee only and the inclusion of detailed audit trails or transaction reports results in a high level of data security and validation.

Other forms of internet banking are effectively on a 'pay anyone' basis, e.g. direct deposit from the school's official account. As robust data security and validations are absent with this type of payment method, this potentially raises the financial risk for the school in relation to:

- the setting up of payee details, and
- the transfer of funds from the official account to valid and accurate payee account(s).

Direct Debit

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.

Types of transactions best suited to Direct Debit

Commitment control over the course of the school year can be managed either by setting aside funds in advance for routine payments (i.e. one standing order for the year for each item, which is progressively reduced by the regular payment) or by the traditional processing of orders and invoices. In both instances, approved program and expenditure budgets should have allowed for the commitment to be incurred.

Expenditure items can be categorised into routine payments or 'one-off', ad hoc payments. Routine payments are regular in amount and/or date due e.g. monthly operating lease, annual insurance premium, while ad hoc payments may be commonplace but incurred on an 'as needs' basis with widely differing dollar amounts e.g. teacher requisites, classroom materials.

This distinction of routine versus ad hoc payments needs to be identified for effective financial management especially in terms of commitment control. When the amount of the routine payment is precisely known in advance e.g. monthly lease payment, and/or the payment date is known in advance e.g. utilities and based on past history, an estimate of the cost can be made.

Establishment of Direct Debit Facility

All suppliers/creditors offering the direct debit facility will require a 'direct debit request' authority from the school. This is usually in a printed form supplied by each creditor for which the direct debit facility is sought. It is important to carefully read and understand the terms and conditions accompanying the direct debit commitment prior to completing and authorising the expenditure. This is essentially a 'service agreement' and should indicate a range of minimum requirements to be provided by the creditor.

Each supplier's terms and conditions may vary from those listed, however they are provided as a guide to enable schools to negotiate and/or confirm minimum standards are in place:

- at least 14 days notice in writing if there are changes to the terms of the drawing arrangements
- information relating to the school's official account be treated confidentially except where required for the purpose of conducting direct debits with your financial institution
- where the due date is not a business day, the creditor will draw from your official account on the nearest business day
- the creditor will at all times attempt to meet the scheduled drawing date as arranged with the school
- the school's ability to alter the drawing arrangements, subject to terms and conditions
- the school's access to appropriate recourse where a drawing is considered to have been initiated incorrectly.

The authority should be signed by the principal and a duplicate copy retained.

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.

Direct Debit information to be retained by School

The following information is to be retained:

- 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
- relevant CASES21 Finance reports.

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.

Establishment of BPAY Facility

The financial institution the school uses for its official account will require a formal registration and authorisation from the school.

As with direct debit, schools should carefully read and consider the terms and conditions accompanying the facility prior to registration.

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.

BPAY Information to be retained by the School

The following information is to be retained:

- 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.
- principal should verify that the details on the tax invoice are identical to the screen print, particularly the biller code and BPAY reference number
- relevant CASES21 Finance reports.

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.

A personal banking package, such as Commonwealth Banks "Netbank", is not recommended as an appropriate school internet banking package due to its primary function being to service personal rather than business based banking. This form of internet banking lacks adequate security (eg single user authorisation) and internal control measures to minimise financial risk and unauthorised access.

The lack of a secure business banking package raises the risk for schools that use this method of payment. Data security is minimal and is totally reliant on the internal control procedures developed and implemented by the school to monitor the authorisation and, accuracy of transactions.

In particular, internal controls surrounding the following process are critical:

School decisions and policy creation

School council should approve in writing the school's decision to use a direct deposit internet banking facility following consideration of the advantages and disadvantages, and internal controls required to be implemented.

This is achieved by developing and gaining endorsement of a Schools Electronic Funds Management policy that deals satisfactorily with all possible internal controls issues. Issues, in particular internal controls surrounding the process are critical to be considered in development of this policy. These include:

- the identification of personnel with administrative/authorisation responsibilities.
  NOTE: The school business manager cannot be nominated as an authoriser even if he or she is a member of the school council.
- The identification of payment authorisers (the Principal and other designated officer).
  NOTE: A single authoriser of payments via internet banking software is a clear breach of the regulations governing the payment of accounts by schools.
- the allocation and security of personal identification number (PIN) information or software authorisation tokens
- the setting up of payee details in CASES21;
- the authorisation transfer of funds from the official account to payee account(s).
- alternative procedures for processing, using the direct deposit facility, for periods of business manager/ES and principal leave or absence

The Schools Electronic Funds Management policy should be reviewed at least once per year to confirm/enhance internal controls.

How to use Direct Deposit

1. Complete all processes for the payment on CASES21

   Creditors

   - entry of purchase orders
   - entry of invoices

   School Level Payroll

   - processing of payroll
2. Generation of payment
3. Printing and signing of payment vouchers
   - all transactions are authorised by the appropriate delegate.
4. Enter transactions into banking software via either:
   - Disk (.aba file)
     - Follow your internet banking software providers instructions for uploading the direct deposit (.aba) file generated in CASES21.
     - Verify the details of the payment against the CASES21 reports (e.g. payment batch)
     - Process the payment through to the authorisation stage
   - Manual
     - Follow your internet banking software providers instructions for the manual entry of data.
     - Verify the details of the payment against the CASES21 reports (e.g. payment batch)
     - Process the payment through to the authorisation stage
5. Two signatories authorise the payment in the banking software
6. Reconcile the payments to CASES21 reports
7. Retain appropriate documentation

Creating the Direct Deposit Disk

Instructions on how to complete the direct deposit transaction are available in Section 3: Creditors and Section 7: Payroll of the CASES21 Finance Business Process Guide.

Direct Deposit information to be retained by the school

The following information is to be retained:

- 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
- relevant CASES21 Finance reports.

3. Electronic Revenue

Schools are 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

Electronic Funds Transfer Point of Sale (EFTPOS)

EFTPOS provides schools with the ability to accept non-cash electronic payments by way of credit and debit card transactions.

Use of EFTPOS allows schools to increase the options and convenience provided to parents/debtors, as well as improves security by reducing the amount of cash handled and kept on school premises.

School decisions and policy creation

Prior to introducing EFTPOS, the school council should give consideration to:

- the cost and benefits for the school of using EFTPOS
- accounting for payments and refunds
- fraud prevention
- information privacy
- EFTPOS security controls.

School council should approve in writing the school's decision for the utilisation of an EFTPOS facility following consideration of the advantages and disadvantages, and internal controls required to be implemented.

If school council recommends the utilisation of an EFTPOS facility, appropriate procedures and practices in the form of a school EFTPOS policy, need to be prepared and formally minuted at school council prior to using the facility. This could be achieved by developing and gaining endorsement of a Schools Electronic Funds Management policy that deals satisfactorily with all possible internal controls issues.

The policy should clearly state what is and also what is not accepted procedure e.g. if the school does not accept EFTPOS transactions to be made by telephone this must be stated in the policy.

Issues to be considered in this policy should include:

- existing bank-imposed restrictions or security measures, such as daily deposit limits
- allocation and security of personal identification number (PIN) information
- a list of personnel with administrative/authorisation responsibilities
- Restriction of 'Cash Out' setting

The Schools Electronic Funds Management policy should be reviewed at least once per year to confirm/enhance internal controls.

To assist in the preparation and development of appropriate school procedures, practices and a policy, consideration of the following information is recommended.

Internal controls

Schools should refer to the publication Internal Control for Schools available on the Financial Management website for information regarding internal control measures applicable to receipting.

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 that need to be considered in relation to EFTPOS include:

- Authorisation and approval of the initial setting up of the facility by school council is required and must be minuted and tabled for school council approval
- 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.

Establishment of EFTPOS facility

The set up of EFTPOS in a school is done in conjunction with a financial institution and schools are advised to compare banks' EFTPOS facility features and fees as these will vary between institutions.

Schools should keep in mind that any EFTPOS fees charged may be dependent on the school's volume of anticipated transactions.

Schools should also determine if any transaction costs will be passed on to the payer, or whether a minimum number of transactions are required to ensure the viability of the EFTPOS facility. Schools should determine if they will implement a minimum or maximum dollar value for transactions after giving consideration to the bank's EFTPOS fee structure.

There is no requirement for a school to set up their EFTPOS facility through the financial institution where the school's official account is being operated. It should be noted though, that a competitive fee structure is available for EFTPOS through the Whole of Government Banking contract currently held by Westpac.

EFTPOS terminals

The configuration settings of the EFTPOS terminal must be specified, approved and minuted by School Council and detailed within the school policy. These would include:

- Receipt Header information
- Receipt Footer information
- Settlement Settings
- Refund limit (changed in conjunction with Bank)

- Maximum transaction limit

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

Any changes to the configuration must be approved and minuted by School Council prior to performing the changes.

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.

Terminals should be located in a secure location which will allow for no unauthorised usage, and ensure privacy for PIN transactions.

Schools should consider if the use of a mobile terminal would be of benefit to school operations, for example, for use in the school uniform shop or at an annual book collection day located separately to the administration building.

Appropriate procedures should be implemented to ensure the security of the terminals during operation and when they are not in use. Arrangements in relation to access to passwords for mobile terminals must be considered. 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

Schools must determine and document if they will accept EFTPOS transactions via the telephone or post.

The school must be approved by the bank as an authorised mail/phone merchant prior to processing transactions of this nature.

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.

Before school council approves the use of phone or mail transactions for receipt of monies, consideration must be given to how the identification of the cardholder will be established, and what documentation will be required to be completed as a record of the phone transaction.

It is recommended that schools develop a proforma to be completed containing information such as:

- cardholders name and address
- card number, expiry date and security code
- transaction date
- identification method and details
- name of staff member processing the transaction and
- invoice details.

Schools must ensure the information collected in order to undertake EFTPOS transactions must only be used for the specified invoice. The proforma should be filed in a secure location with restricted access.

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.

Processing transactions

Schools should only process transactions to accept school invoice payments i.e. family charges, sundry debtors, trading operation payments etc. Schools are not to undertake transactions which provide 'cash' to the customer as part of the transaction.

The maximum amount of a credit/debit card transaction is determined by the cardholder's limit unless school council policy determines a maximum transaction limit for the school.

Customers have the option of using a "Pen" (Signature) or "PIN" (Personal Identification Number) to authorise transactions. 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

Schools 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

If it is determined at the time of the transaction and **prior to entering the receipt on CASES21**, that an error has occurred, for example an incorrect amount is processed, schools should "void" or "refund" the transaction ***via the EFTPOS terminal***. Schools should refer to the instructions provided in the EFTPOS facility user guide to ensure that this is processed correctly.

Key internal controls relating to the reversal of incorrect EFTPOS transactions include:

- 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 proforma 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.
- schools should develop a refund request proforma 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
    - 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.

Manual transactions

Whilst DEECD would deter manual processing to limit exposure to the risks associated, there may be instances when the EFTPOS facility will be offline, for example when electronic communication with the bank is unavailable.

In these instances the bank will have set a transaction floor limit for each school, which is the maximum offline transaction allowed to be undertaken without contacting the bank for authorisation. When the system is offline, schools may approve only credit card transactions and only up to their floor limit.

Debit card transactions must not be performed when the school's EFTPOS facility is offline as a zero floor limit applies to debit cards.

An authorisation must be obtained from the bank for all transactions which are greater than the school's floor limit.

If school council deems that its floor limit is too high/low the school should negotiate a more suitable limit with the bank.

If the bank has provided a manual card reader this should be used to complete offline credit card transactions with reference to any instructions provided by the financial institution. If a manual card reader is not available (they are not mandatory), the school should complete the proforma used for phone transactions and process the transaction as soon as connection to the financial institution is restored.

Banking

There are three factors schools will need to consider when determining how to process EFTPOS receipts in CASES21 Finance either via a normal receipt batch that contains cash and/or cheques, or as a separate EFTPOS only receipt batch. These factors are:

- a Settlement* must be run on the EFTPOS terminal at the end of each day
- the volume of EFTPOS transactions undertaken by the school
- how often banking is undertaken.

Below are options schools can adopt to process their EFTPOS receipts.

It is recommended that schools with a large volume of transactions should consider using Option 1 or 2. Schools with a small volume of transactions can utilise any of the Options.

Option 1

- 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.*

Using this option provides schools with clear and current information regarding EFTPOS transactions in case of any enquiries.

It is also an effective internal control measure reducing the risks of fraud or misappropriation of funds.

Option 2

- Schools include EFTPOS receipts in a normal receipts batch with cash and/or cheque receipts that is updated at the end of each day. This option helps to reduce the number of batches opened each day
- The Settlement* on the terminal is also performed at the same time as the batch is updated. The *EFTPOS* total (Batch total less Bank Deposit Slip total) should match the Settlement* total (unless adjustment is required for a refund)
- *On the Bank Reconciliation, the EFTPOS total for that date 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. It is **strongly recommended** that schools perform settlement each day at a time determined by the school.

EFTPOS information to be retained by the school

The following information is to be retained:

- 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
- proforma/documents containing transaction details
- merchant copies of EFTPOS terminal receipts, voided/cancelled receipts and settlement documents
- applicable CASES21 reports
- daily EFTPOS reconciliation reports and documentation in support of refunds and/or adjustments.

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.

School decisions and policy creation

Prior to introducing BPAY, the school council should give consideration to:

- the cost and benefits for the school of using BPAY
- accounting for payments and refunds
- fraud prevention
- information privacy.

School council should approve in writing the school's decision for the utilisation of BPAY following consideration of the advantages and disadvantages, and internal controls required to be implemented.

If school council recommends the utilisation of BPAY, appropriate procedures and practices in the form of a school BPAY policy, need to be prepared and formally minuted at school council prior to using the facility. This could be achieved by developing and gaining endorsement of a Schools Electronic Funds Management policy that deals satisfactorily with all possible internal controls issues. The policy should clearly state what is and also what is not accepted procedure e.g. detailing the schools process for applying receipts to invoices should be stated in the policy.

The Schools Electronic Funds Management policy should be reviewed at least once per year to confirm/enhance internal controls.

Internal controls

To assist in the preparation and development of appropriate school procedures, practices and a policy, schools should refer to the publication Internal Control for Schools available on the Financial Management website for information regarding internal control measures applicable to receipting.

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.

Information on establishing BPAY facility for families, how to use BPAY and what is to be retained by the school is available in Section 1: Families of the CASES21 Finance Business Process Guide.

Third party internet revenue collection

Schools can engage a third party company or product to facilitate electronic payments by way of credit and debit card transactions through a secure internet payment gateway.

Use of this form of revenue collection allows schools to increase the options and convenience provided to parents/debtors, as well as improves security by reducing the amount of cash handled and kept on school premises.

School decisions and policy creation

Prior to introducing a third party company or product, the school council should give consideration to:

- the cost and benefits for the school
- accounting for payments and refunds
- fraud prevention
- the validity of the company to be engaged
- information privacy
- website security controls
- terms and conditions of use of the service

School council should approve in writing the school's decision for the utilisation of a third party company or product following consideration of the advantages and disadvantages, and internal controls required to be implemented.

If school council recommends the utilisation of a third party company or product, appropriate procedures and practices in the form of a school third party company or product policy, need to be prepared and formally minuted at school council prior to using the facility. This could be achieved by developing and gaining endorsement of a Schools Electronic Funds Management policy that deals satisfactorily with all possible internal controls issues. The policy should clearly state what is and also what is not accepted procedure e.g. detailing the schools process for applying receipts to invoices should be stated in the policy.

The Schools Electronic Funds Management policy should be reviewed at least once per year to confirm/enhance internal controls.

Internal controls

To assist in the preparation and development of appropriate school procedures, practices and a policy, schools should refer to the publication Internal Control for Schools available on the Financial Management website for information regarding internal control measures applicable to receipting.

The internal controls that need to be considered in relation to the use of a third party company or product include:

- authorisation and approval of the initial setting up of the facility by school council is required and must be minuted and tabled for school council approval
- the website security controls identified and recorded
- documentation kept by the school confirming all transactions, void receipts, refunds, 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 a website access user register outlining the name of the school user, their unique ID (if one exists) and the website functions they are authorised to perform
- register of void or refund transactions
- reconciliation of monthly statement received from the third party company or product with CASES21 transaction records
- reconciliation of daily settlement statements with CASES21 transactions.