



St Brendan's School
1 Ti Tree Road, Dunnstown 3352
Tel: 0353 347604 Fax: 0353 347042



St Mary's School
131 Powells Road, Clarkes Hill 3352
Tel: 0353 345280 Fax: 03534 5445

PARISH PRIEST: Fr Shane Mackinlay
PRINCIPAL: Mr Chris Kavanagh

FRAUD PREVENTION POLICY (PURCHASING POLICY)

Ratified: 31st July 2015

Review: July 2019

Appendix 1: Staff re-imburement form
School Management Checklist for Fraud Prevention



St Brendan's School

1 Ti Tree Road, Dunnstown 3352

Tel: 0353 347604 Fax: 0353 347042

St Mary's School

131 Powells Road, Clarkes Hill 3352

Tel: 0353 345280 Fax: 03534 545280

RATIONALE:

To ensure that fraudulent activities do not occur in Diocesan schools.

DEFINITION:

For the purposes of this policy fraud is the obtaining of money or a financial advantage, for yourself, or for another person, through dishonesty or deception. Fraudulent activity may include the physical theft of monies or other property, deliberate falsification of statements or documents, concealment, improper use of information, conflict of interest and destruction or use of falsified documentation. Fraud prevention is essential to protect an organisations assets, revenue and expenditure.

POLICY STATEMENT:

We are committed to the protection of our assets, revenue and expenditure to ensure that its assets and income are used for the purpose for which they were intended and report any incident where this is not the case.

PRINCIPLES:

- 1.0** The fraud prevention and reporting policy and procedures are intended to cover all individuals and organisations associated with the school to prevent and detect fraudulent activity. The school is committed to communicating and reinforcing the School Fraud Prevention and Reporting Policy and Procedures to all staff and volunteers. All individuals and organisations associated with the school are expected to act with integrity and honesty and reflect the organisation's values.
- 2.0** It is the responsibility of the Principal, Governing Authority and School Advisory Council/Board/Finance Committee to detect fraudulent activities. They are to ensure appropriate and effective preventative internal control systems are in place. The Governing Authority, all members of the School Advisory Council/Board/Finance Committee and Principal should ensure mechanisms are in place to:
 - Identify, assess, control and monitor the risk of fraud
 - Educate employees and volunteers about fraud prevention and protection
 - Facilitate the reporting of suspected fraudulent activities

All members of staff and volunteers engaged in financial or non-financial activities share responsibility to prevent, detect and report fraudulent behaviour in their areas of responsibility.

REFERENCES:

1. School Management Commitment and Approach to Fraud Prevention

- 1.1 School management should communicate and make available the Fraud Prevention and Reporting Policy and Procedures to all school staff that assist with school assets.
- 1.2 The school should conduct training for staff and volunteers in the Fraud Prevention Procedures and outline their responsibilities to report any suspected fraud. This may be included in induction programs for new staff.
- 1.3 The Governing Authority and Principal should ensure that the Fraud Prevention Policy and Procedures are followed by all school staff and that there is adequate supervision and review of processes and financial statements.
- 1.4 The school must clearly define the reporting procedures for their school communities and employees to report cases of suspected fraud to the Governing Authority.
- 1.5 The Governing Authority and Principal should support people who report fraudulent activities.
- 1.6 The school should communicate to their school communities and employees their commitment to pursuing and taking appropriate action against the person(s) responsible for any fraudulent activity.
- 1.7 The Governing Authority and Principal may choose to investigate Fidelity Guarantee Insurance.

2. School employee and volunteer practices

- 2.1 Ensure pre-employment checks of employees and volunteers are carried out including: verification of identity, criminal record checks, verification of qualifications and reference checks.
- 2.2 Develop staff role descriptions that include:
 - 2.2.1 Authorisation levels where necessary,
 - 2.2.2 The duty to report financial discrepancies and suspected fraud to management,
 - 2.2.3 The duty not to disclose any private financial information to a third party
- 2.3 Regularly educate staff on Fraud Prevention Procedures – include in staff/team meetings.
- 2.4 Develop a procedure for leave accumulation where appropriate.
- 2.5 There is a defined limit for the maximum amount of cash that can be held at the school at one time.
For example: bank money collections above \$500 within 48 hours.
- 2.6 Restrict access to the school safe and financial documents to nominated school management.
- 2.7 Ensure school keys are stored out of sight in a locked cabinet or safe.
- 2.8 The key to the safe should be restricted to nominated school managers.
- 2.9 Develop a school asset register listing all physical and financial assets owned by the school.
- 2.10 Conduct regular stock takes to keep the asset register current.

- 2.11 Develop budget forecasts for regular business operations. Compare the budget and actual financial performance for discrepancies and report any differences.
- 2.12 Identify school operations and business that are most at risk of fraud including but not limited to: cash, access to bank accounts and assets that could be easily removed.
- 2.13 From the high risks identified, assess the likelihood and consequences of fraud occurring.
- 2.14 Determine appropriate procedures and risk controls to be put into action to prevent these risks occurring.
- 2.15 Hold regular school meetings to discuss financial reports and budgets and record the minutes of the school meetings.
- 2.16 Develop written procedures for the financial authorisation limits for all staff including: cheques, credit cards, investments, purchases and petty cash.
- 2.17 Obtaining quotes and the issuing of purchase orders for all work is an essential part of a fraud prevention regime. The official school purchase order book should be used for all purchases of goods and services greater than \$75 in total (not per individual item), excluding Goods and Services Tax (GST). The following guidelines are recommended for obtaining quotes and tenders:
 - (a) A minimum of **one written quote** should be obtained for purchases of between \$2,000 and \$5,000. The written quotes should be maintained on file.
 - (b) A minimum of **two written quotes** should be obtained for purchases between \$5,000 and \$15,000. The written quotes should be maintained on file.
 - (c) A minimum of **three written quotes** should be obtained for capital purchases between \$15,000 and \$100,000, and non-capital purchases between \$15,000 and \$50,000. The written quotes should be maintained on file.
- 2.18 Ensure controls for authorisation limits are in place (eg. Maximum limits of cheque accounts and credit card accounts are confirmed in writing with the bank).

Develop written procedures for all financial areas including: money collection, money counting, banking, cheques, credit cards, contractor payment, reconciliation and audits etc.

- 2.20 Ensure all cheques have two signatories with the appropriate authority levels.
- 2.21 Ensure cash counting and banking is signed off by at least two people and is supervised by a senior member at all times.
- 2.23 Regularly record financial transactions so that unauthorised transactions are immediately identified.
- 2.24 Reconcile all cheques, credit cards, investments and bank accounts with statements and ensure that the reconciliation is reviewed and signed off by an authorised person.
- 2.25 The Governing Authority /Principal should ensure that all staff are complying with the fraud prevention procedures through supervision and review of financial records.

3. Segregation of duties (where possible)

- 3.1 Segregate the duties of accounting reconciliation review and the accounting functions.
- 3.2 Ensure bank statements, investments, credit cards and cashbooks are reconciled by a separate person with authority to do so, in a timely manner to detect discrepancies.

- 3.3 Segregate the duties of money collecting/payments to the duties of the person providing the accounting functions.
- 3.4 Ensure the Principal supervises the administration of school funds.

4. School Data Protection Procedures

- 4.1 Ensure files containing financial and/or personal information are stored in lockable cabinets.
- 4.2 Maintain a key register/security card register to control key access. Review the register when personnel changes occur.
- 4.3 Ensure filing cabinet keys for cabinets containing financial and/or personal information are kept in a lockable safe and signed out and in after use.
- 4.4 Ensure computers are protected by passwords and locked whilst not in use – implement a timed password security process to reduce access to computers if staff are called away from their desk.
- 4.5 Ensure computer Firewalls and Anti-virus software are installed and operational on all computer equipment and updated regularly.
- 4.6 Maintain all financial and/or personal information in house and prohibit the use of portable back-up devices such as data sticks and portable hard drives, unless expressly required for business continuity purposes.
- 4.7 If financial and/or personal records are to be stored off-site for business continuity purposes, ensure that information is backed up by a senior member of staff and stored in a secure data storage facility.
- 4.8 When required to dispose of information, ensure paper documents are shredded and electronic records are either:
 - Shredded via a data shredder
 - Degaussed (de-magnetising magnetic media for example, hard drives) or
 - Physically destroyed (eg. Incineration or pulverisation) (this should be undertaken by a suitably qualified individual in accordance with EPA guidelines)
- 4.9 Ensure that data protection procedures are reviewed for effectiveness and amended if deemed necessary by the Governing Authority or Principal.

5. Review process

- 5.1 Develop a school Fraud Prevention and Control review checklist and complete at regular, nominated intervals (*At least annually*).
- 5.2 Conduct regular internal audits of the following control areas:
 - Account balances and accounting records
 - School and Personnel practices
 - Data and data protection practices
- 5.3 The Governing Authority and Principal should review both the internal and external audit reports and investigate the findings.
- 5.4 Where current controls are deemed ineffective or out-dated, implement the revised risk controls.

6. Issue Management Process

- 6.1 Suspected fraudulent activity should be reported to the Principal/Catholic Education Office to be investigated and substantiated.
- 6.2 If substantiated, the fraudulent activity must be reported to the Governing Authority, the Director of Catholic Education and to Victoria Police.

Reference: Catholic Church Insurances Risk Management Sample Fraud Prevention Policy

Appendix 1

STAFF RE-IMBURSEMENT REQUEST FORM

Payable To: _____

Date: _____

Amount: _____

Invoice/s Attached for:

Principal Authorised: _____

PLEASE SUPPLY BANK DETAILS FOR PAYMENT

BSB: _____

Account No: _____



St Brendan's School
 1 Ti Tree Road, Dunnstown 3352
 Tel: 0353 347604 Fax: 0353 347042

**BUNGAREE PARISH
 SCHOOLS**
 PARISH PRIEST: Fr Shane Mackinlay
 PRINCIPAL: Mr Chris Kavanagh



St Mary's School
 131 Powells Road, Clarkes Hill 3352
 Tel: 0353 345280 Fax: 03534 545280

School Management Checklist to Fraud Prevention

The following checklist is intended to provide general information to assist schools to assess and reduce the risk of fraud. Please note that this is not an exhaustive checklist of all possible procedures or controls you might use to prevent fraud.

Understanding the risks that your school is exposed to will assist you to put in place measures that reduce the incidence of fraud.

The school fraud prevention policy should be consistent with best practice prevention programs and standards. The school may need to seek professional advice for specific fraud prevention measures.

Where the school answers the question with a “no”, further investigation of the risk and possible control measures should be identified and implemented.

School Management Commitment and Approach to Fraud Prevention		Yes	No
1.1	Do school management communicate and make available the Fraud Prevention and Reporting Policy and Procedures for staff and volunteers that assist with school assets?		
1.2	Do staff and volunteers receive training in Fraud Prevention Procedures and their responsibility to report any suspected fraud? (eg. is this included in the induction programs for new staff?)		
1.3	Do school management ensure that the Fraud Prevention and Reporting Policy and Procedures are followed by all school staff by providing supervision and review of processes and financial statements?		
1.4	Are there clearly defined reporting procedures in place for employees to report cases of suspected fraud to school management?		
1.5	Are there procedures in place to protect individuals who report fraudulent activities?		
1.6	Is the school's commitment to pursuing and taking legal action against the person(s) responsible for any fraudulent activity communicated to employees?		
1.7	Is there adequate Fidelity Guarantee Insurance held for the school's operations (if appropriate)?		

School employee and volunteer practices		Yes	No
2.1	Are pre-employment checks of employees and volunteers carried out including: verification of identity, criminal record checks, referee checks, and verification of qualifications?		
2.2	Do staff role descriptions include:		
2.2.1	Authorisation levels where necessary		
2.2.2	The duty to report financial discrepancies or suspected fraud to management		
2.2.3	The duty not to disclose any private financial information to a third party.		
2.3	Are staff regularly educated on Fraud Prevention Procedures?		
2.4	Is there a procedure for leave accumulation?		
2.5	Is there a defined limit for the maximum amount of cash that can be held at the school at one time? eg are money collections over \$500 banked within 48 hours?		
2.6	Is access to the school safe and financial documents restricted to nominated school management?		

2.7	Are school keys stored out of sight in a locked cabinet or safe?		
2.8	Is the key or code to the safe restricted to nominated school managers?		
2.9	Is there a school Asset Register listing all physical and financial assets owned by the school?		
2.10	Are regular stocktakes conducted to keep the asset register current?		
2.11	Are school budgets forecasted for regular business operations?		
2.12	Are the budgets and actual financial performance compared for discrepancies and reported?		
2.13	Are all high risk areas for fraud identified within the parish operations and business including, but not limited to: cash, access to bank accounts and assets that could easily be removed?		
2.14	From the high risks identified, is the likelihood and consequences of the risk of the fraud assessed?		
2.15	Are appropriate procedures and risk controls put into action to prevent these risks occurring?		
2.16	Are regular school meetings conducted to discuss financial reports and budgets?		
2.17	Are the minutes of the meetings recorded?		
2.18	Are procedures written for the financial authorisation limits for all staff including: cheques, credit cards, investments, purchases, petty cash etc?		
2.19	Are controls for these limits in place? (eg. maximum limits of cheque accounts and credit cards are confirmed in writing with the bank)		
2.20	Are written procedures kept for all financial areas including money collection, money counting, banking, Cheques, credit cards, contractor payments, reconciliation, and audits etc?		
2.21	Do cheques have two signatories/passwords for EFT transactions with the appropriate authority levels?		
2.22	Are cash counting and banking signed off by at least two people and supervised by a senior school leader at all times?		
2.23	Are financial transactions recorded regularly so that unauthorised transactions are Immediately identified?		
2.24	Are reconciliations conducted for all cheques, credit cards, investments and bank accounts with discrepancies reported?		
2.25	Are there written procedures for fraud reporting, investigation and disciplinary actions?		
2.26	Are staff aware of their responsibilities and accountable for their actions?		
2.27	Do school management ensure that all staff are complying with the fraud prevention procedures through supervision and review of financial records?		

Segregation of duties (where possible)		Yes	No
3.1	Are the duties of accounting reconciliation review and the accounting functions segregated?		
3.2	Are bank statements, investments, credit cards and cashbooks reconciled by a separate person in a timely manner to detect discrepancies?		
3.3	Are the duties of money collecting/payments segregated to the duties of the person providing the accounting function?		
3.4	Is the administration of school funds supervised by the Principal?		

School Data Protection Procedures		Yes	No
4.1	Are files containing financial or personal information stored in lockable two hour fire rated cabinets?		
4.2	Is a key register/security card register maintained to control key access?		
4.3	Is the register reviewed when personnel changes occur?		
4.3	Are filing cabinet keys for cabinets containing financial and/or personal information kept in a lockable key safe and signed out and in after use?		
4.4	Are all computers protected by passwords and locked whilst not in use with a timed password security process to protect computers if staff are away from their desk?		
4.5	Is all computer equipment installed with Firewalls and Antivirus software and regularly updated?		
4.6	Is all school financial or personal information contained in-house?		
4.7	Is the use of portable backup devices such as data sticks and portable hard drives prohibited, unless expressly required for business continuity purposes?		
4.8	If financial and/or personal records are to be stored offsite for business continuity purposes, is the information backed up by a senior member of staff and stored in a secure data storage facility?		
4.9	Are paper documents and electronic records shredded when required to dispose of information, by any of the following ways: <ul style="list-style-type: none"> • Shredded via a data shredder? • Degaussed (demagnetising magnetic media for example hard drives)? • Physically destroyed (eg. Incineration or pulverisation etc? - this should be undertaken by a suitably qualified individual in accordance with EPA guidelines) 		
4.10	Are data protection procedures reviewed for effectiveness and amended if deemed necessary by the Principal?		

Review Process		Yes	No
5.1	Is there a school Fraud Prevention and Control Review checklist completed at least annually?		
5.2	Are regular internal audits conducted for the following control areas? <ul style="list-style-type: none"> • Account balances and accounting records • School and Personnel practices • Data and data protection practices 		
5.3	Are the internal and external financial audit reports reviewed by school management and the findings investigated?		
5.4	Where current controls are deemed ineffective or outdated, are revised risk controls implemented?		

Issue Management Process		Yes	No	NA
6.1	Has suspected fraudulent activity been reported to the Principal/Catholic Education Office to be investigated and substantiated?			
6.2	If substantiated, the fraudulent activity was reported to the Governing Authority, the Director of Catholic Education and to Victoria Police.			

Reference: Catholic Church Insurances Risk Management Sample Fraud Prevention Policy