

<b>Preventing Fraud</b>	
Reference: <b>FP09</b>	Effective date: 1 June 2012
Page no: <b>1 of 3</b>	Approved: 12 Sept 2022
Last revision 26 Aug 2022	Next revision due: Aug 2024



## Introduction

The organisation requires a policy and procedures to avoid or deal with fraud, theft and corruption. This concerns both potential internal offences and attempts to commit offences by project or other partners.

## General

If any attempted, suspected or proven fraud occurs, including those involving project partners, an investigation must be carried out and a report submitted to the Chief Executive. The initial investigation will normally be internal, but external bodies may be involved if necessary. The Chief Executive should report cases to the appropriate authorities (eg police) and inform the Board of Trustees. If the Chief Executive is suspected or implicated in fraud, then the matter must be notified directly to the chair of trustees or other authority (see policy GN22 – Whistleblowing).

Where the fraud involves a member of staff the Disciplinary procedure (GN05) should be followed. Appropriate action should be taken to ensure that similar frauds cannot be repeated.

## Fraud risks and controls

Potential risk	Controls
----------------	----------

### Accounts Payable

Fictitious invoices entered and paid.	All invoices authorised by a budget holder before payment can be made.
Blank cheques stolen and used for unauthorised transactions.	Cheque book kept secure by finance team. All cheques require two authorised signatures.
Cheques stolen before they reach recipient.	Payments made by BACS as far as possible. Bank account and supplier accounts checked and reconciled on a monthly basis.
Copy invoices used to support fraudulent claim for payment.	All invoices must be authorised by a budget holder. A photocopy of a signature will not be accepted.
Cheques issued using a forged signature.	Company bankers have responsibility for checking that all signatures are genuine.
Funds stolen from petty cash.	All petty cash claims to be authorised by a budget holder. Petty cash balance counted on a monthly basis and reconciled to the accounting system.
Collusion with suppliers to invoice and pay extra amounts and misappropriation of the excess funds.	Purchase invoices to be supported by an authorised purchase order where appropriate. All invoices authorised by a budget holder before payment can be made.

<b>Preventing Fraud</b>	
Reference: <b>FP09</b>	Effective date: 1 June 2012
Page no: <b>2 of 3</b>	Approved: 12 Sept 2022
Last revision 26 Aug 2022	Next revision due: Aug 2024



## Purchasing

Fictitious invoices created and entered on to finance system. Payments later diverted for personal use.	Purchase invoices checked to purchase order and delivery notes where available. Invoices authorised by budget holder before payment can be made.
Personal purchases charged to company.	Purchase invoices supported by approved purchase order where possible. Invoices authorised by budget holder before payment can be made.
Personal purchases made using company credit card.	All credit card transactions authorised by budget holder, supported by an approved purchase order where possible.
Purchase of unauthorised goods through expense claims to avoid purchase order and authorisation processes.	Expenses to be authorised by budget holder.

## Accounts Receivable

Funds received from customers re-directed into a personal account.	Monthly 'Cheques received' log prepared by the person responsible for opening mail. List agreed to bank receipts for the month.
Cheques deposited but not recorded, fraudulent payment for same amount entered and funds diverted.	All transactions reconciled from bank statement to accounting system on a monthly basis.
Customer account closed and balance written off as bad debt. Funds misappropriated.	All credit notes and bad debt write off's to be authorised by senior management.
Fail to deposit full funds in the company's bank account and divert surplus funds.	Aged debtors listing to be produced and reviewed monthly. Old balances to be followed up through issue of statements and debt chasing.

## Payroll, expense claims and benefits

Fictitious employees entered on payroll and payment diverted to personal account	Payroll processing carried out by 2 people. Salary payments authorised by Chief Executive.
Employee paid twice in one month.	Payroll control accounts reconciled on a monthly basis.
Payroll payments manipulated so an employee receives more pay than they should.	Payroll processing carried out by 2 people. Salary payments authorised by Chief Executive.
Employee remains on payroll after leaving date and further payments made against their payroll reference.	Payroll processing carried out by 2 people. Salary payments authorised by Chief Executive.



<b>Preventing Fraud</b>	
Reference: <b>FP09</b>	Effective date: 1 June 2012
Page no: <b>3 of 3</b>	Approved: 12 Sept 2022
Last revision 26 Aug 2022	Next revision due: Aug 2024

Falsify employee holiday and sick records.	All leave authorised by line manager. Sickness records maintained by HR. HR assist in preparation of monthly payroll.
Identity theft through access to confidential employee records.	Restricted access to employee records.

### **Bank accounts**

Unauthorised payments made from the business bank account.	Input and authorisation duties split. Payments can only be authorised by a senior manager (see FP01 for a list).
--	--

### **Fixed assets**

Business assets removed and used for personal use.	Fixed asset register checked on an annual basis.
Assets deleted from fixed asset records then disposed of for personal financial gain.	Fixed asset register checked on an annual basis.
Take business property for personal use or sale.	Fixed asset register checked on an annual basis.