

## FRAUD CONTROL: INTERNATIONAL PROGRAMME PROCEDURE

### CONTENTS

PURPOSE .....	2
SCOPE.....	2
DEFINITIONS AND ACRONYMS .....	2
RELATED DOCUMENTS.....	2
PROCEDURE .....	3
Risk Assessment .....	3
Preventative Controls.....	4
Detecting and Reporting of Fraudulent Activities .....	5
COMPLIANCE STRATEGY .....	6

## PURPOSE

Family Planning Australia (FPA) works to achieve the highest standards of honesty and integrity and comply with all relevant legislation and regulations.

FPA takes a zero-tolerance approach to all forms of fraud and is committed to conducting organisational and program management in a transparent and accountable manner to support good governance.

For all international development activities in which it takes part, FPA will take all measures necessary to prevent all forms of fraud, bribery and corruption from occurring in operations and the projects it supports.

## SCOPE

All FPA staff, board of directors, contractors, students and volunteers engaged in international development program delivery.

All in-country partners and organisations contracted to deliver FPA international projects and their staff, contractors and volunteers.

## DEFINITIONS AND ACRONYMS

Term	Meaning
<b>Fraud</b>	Dishonestly obtaining a benefit, or causing a loss, by deception or other means. Fraud includes theft of funds or assets, misappropriation of funds, falsifying invoices or signatures, unlawful use of equipment, material or services, unauthorised disclosure of confidential information or wrongfully using intellectual property
<b>Fraud control strategy</b>	Is the plan for how fraud will be managed or controlled in FPA, documented in the FPA risk register
<b>Fraud risk assessment</b>	Identifies fraud risks and corresponding controls to minimise or mitigate the identified risks

## RELATED DOCUMENTS

For further information, refer to:

- DFAT [Fraud Control Toolkit](#) for Funding Recipients
- Family Planning Australia policies and procedures:
  - Fraud Control and Anti-Corruption Policy – International Programme
  - Code of Conduct and Ethics
  - Delegations policy
  - Fixed asset management policy
  - Investment policy
  - Petty cash management cash handling and receipting policy
  - Purchasing policy
  - Revenue recognition and receipting procedure

- Foreign exchange policy
- Travel policy
- International travel and security policy
- IT and cloud systems usage policy
- Risk Management Policy
- Data Security and Handling Standards Policy
- Counter Terrorism policy
- Whistleblower policy
- Incident management policy
- Recruitment and Selection Policy
- Learning and development procedure
- Partner Capacity Checklist including Financial Assessment form.

## PROCEDURE

### Risk Assessment

FPA undertakes organisational and project risk assessments to identify fraud risks and mitigating strategies to prevent and detect fraud.

- i. An organisational risk assessment is conducted and documented in the FPA risk register in accordance with the FPA Risk Management Policy. This forms the Fraud Control Strategy.
- ii. The risk register is reviewed at least monthly by the relevant Executive and CEO, reported quarterly to the FPA Audit and Risk Committee and annually to the Board.
- iii. Project specific fraud risk assessments are conducted on all DFAT funded projects within one month of the commencement of the project and documented as part of the project plan. The risk assessment is conducted by all staff included in the project team. The fraud risk assessment and strategy must contain project specific fraud prevention, detection, investigation and reporting processes and procedures.
- iv. Project specific risk assessments are reviewed and updated on a six-monthly basis by the Project Lead and the Manager International Programme to ensure risks and treatment are appropriate.
- v. Prior to engaging with international partners, a partnership assessment is conducted to ensure that the partner has appropriate fraud prevention strategies and financial policies and procedures in place. This is documented in the Partner Capacity Checklist including Financial Assessment form.
- vi. Prior to signing a contract or MoU with international partners, all organisations are checked against the Australian government lists related to terrorism financing (see Counter Terrorism policy).

## Preventative Controls

FPA will implement a range of preventative strategies at an organisational and project level.

1. Expectations of staff are documented and implemented according to defined policies and procedures including the
  - Fraud Control and Anti-Corruption Policy – International Programme
  - Family Planning Australia Australia Code of Conduct and Ethics
  - Delegations policy
  - Fixed asset management policy
  - Investment policy
  - Petty cash management cash handling and receipting policy
  - Purchasing policy
  - Revenue recognition and receipting procedure
  - Foreign exchange policy
  - Travel policy
  - IT and cloud systems usage policy.
2. Financial controls are implemented to ensure
  - all financial transactions are recorded in financial systems, including detailed records of expenditure against relevant budget lines
  - separation of duties, such as separation of accounts payable and accounts receivable and to ensure that staff approving expenditure must not be in a position to benefit from that expenditure.
  - regular monitoring and investigating variances from budget
  - service delivery is substantiated before invoices are paid
  - two cheque signatories for all payments (EFT, direct debit, cheque)
  - maintenance and regular review of asset registers
  - annual audit of systems and financial statements by qualified auditors
3. Mandatory training is provided on fraud control and anti-corruption at orientation and on an annual basis to relevant staff (refer to Learning and development procedure). This is recorded within ELMO in the individual employee record and a copy of the training certificate.
4. Data safety and security safeguards are implemented to ensure that data is protected from accidental or intentional unauthorised modification, destruction or disclosure (refer to Data Security and Handling Standards Policy).
5. FPA undertakes a criminal record check and referee checks for any person offered employment by the organisation as part of pre-employment screening (refer to Recruitment and Selection Policy)
6. Confirmation of appointment to this position will be conditional upon a satisfactory Criminal Record Check.
7. Staff responsibilities and expectations are clearly articulated in position descriptions, performance plans recorded on ELMO and in project plans.
8. Expectations of implementing partners, contractors and consultants are documented with the inclusion of fraud and anti-corruption clauses in the memorandum of understanding or contract. This includes
  - a. provision of source documentation such as receipts, invoices, statements and vouchers to validate expenditure
  - b. confirmation of fund transfers received from partners
  - c. analysis of partner's audited financial statements

- d. ongoing review of project financial performance against budget to detect any significant variations

## **Detecting and Reporting of Fraudulent Activities**

1. FPA will identify and implement a range of strategies to detect fraudulent activities across the organisation including:
  - all international travel expenses claims are reviewed and verified
  - conducting audits of leave accruals and hours worked
  - reviewing international and domestic telephone bills monthly to determine whether charges are appropriate
  - monitoring and acquitting expenditure through monthly reconciliation of invoices/statements by delegate
  - maintaining vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the officer using the vehicle
  - auditing expense reports and credit card charges regularly to determine whether charges are appropriate
  - ensuring access to the FPA network is through two factor authentication with passwords updated every 90 days
  - ensuring an audit trail (data log) of changes made to the IT system, including when changes were made and by which user
  - maintaining ICT access logs and reviewing periodically
  - conducting random process checks regularly
  - conducting internal audits
2. Should fraud be detected or suspected, it must be reported immediately to the CEO through the FPA Incident management policy.
3. FPA Whistleblower policy documents the process for any person, including but not limited to employees, volunteers, contractors, suppliers or members of the public who detect, become aware of or have reasonable grounds for suspecting improper conduct associated with FPA to raise concerns without being subject to discriminatory treatment. The Whistleblower policy is available on the FPA website, and a link included in partner MoUs.
4. Any potential fraud with DFAT funded projects must be reported within five business days to the Fraud Control Section at [fraud@dfat.gov.au](mailto:fraud@dfat.gov.au) using the Suspected or Detected Fraud Reporting form. FPA will follow the DFAT direction for handling suspected fraud and will ensure DFAT is informed of the progress and resolution of any investigation within 5 business days of any further information request by DFAT.
5. FPA will report detected fraud to the appropriate law enforcement agency. Before doing this, FPA will consider if reporting the incident could:
  - compromise the safety of a person's life or
  - significantly impact on them to an extent which would result in undue hardship or
  - result in a disproportionate response to the circumstances of the fraud (taking into account remedial actions already taken)

If the above factors exist, FPA will liaise with the Fraud Control Section to seek an exemption from police reporting by sending an email to [fraud@dfat.gov.au](mailto:fraud@dfat.gov.au).

## COMPLIANCE STRATEGY

<b>ITEM</b>	<b>AUDIT FREQUENCY / EVIDENCE</b>	<b>PERSON RESPONSIBLE AND DESIRED OUTCOME</b>
Complete DFAT Fraud self-assessment checklist	Every 3 years	Director Finance and Director Planning, Education and International Programme