

TACKLING EXTERNAL FRAUD



POLICY FRAMEWORK

1. External fraud is where a third party, such as a business, individual or organised crime group, steal money from a government organisation either by obtaining payments to which they are not entitled or by keeping money they should pay over to the government organisation.

Any such action, or attempted action, to defraud PLR of public funds is unacceptable and will not be tolerated by the Registrar.

2. The Fraud Act 2006 includes three classes of Fraud:

Fraud by false representation

- (1) A person is in breach of this section if he (or she):
 - (a) Dishonestly makes a false representation, and
 - (b) intends, by making the representation:
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss.
- (2) A representation is false if:
 - (a) it is untrue or misleading, and
 - (b) the person making it knows that it is, or might be, untrue or misleading.

Fraud by failing to disclose information

A person is in breach of this section if he:

- (a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
- (b) intends, by failing to disclose the information:
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss.

Fraud by abuse of position

- (1) A person is in breach of this section if he:
 - (a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
 - (b) dishonestly abuses that position, and
 - (c) intends, by means of the abuse of that position:
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss.

- (2) A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

For an offence to have occurred a person must have acted dishonestly and with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of loss) on another.

3. Identifying Types of possible external Fraud at PLR

- (1) Fraud by false representation:
 - Impersonating an eligible author and registering for PLR
 - Impersonating a registered author and changing personal details
 - Amending a PLR cheque before paying in to bank/building society
 - Unauthorised use of PLR's credit or Government Procurement cards

- (2) Fraud by failing to disclose information:
 - Failure to disclose other contributors
 - Failure to notify PLR office of changes in eligibility criteria ie residence

- (3) Fraud by abuse of position:
 - Abuse of privilege where 'Power of Attorney' is in place
 - A Librarian or LMS system supplier deliberately manipulating loans data prior to transmission to PLR office from a sample library authority

4. Roles and Responsibilities

(See 'Tackling Internal Fraud' section)

5. PLR's External Fraud Response Plan

- a) If you suspect or discover fraud it must be reported immediately to your manager who will in turn report to the Registrar. The Registrar will take immediate personal charge of any relevant documentation and will normally report the matter to the police.
- b) The fraud must be stopped at the earliest opportunity. Immediately block access to online account and inform staff to direct any calls/communications from person suspected of fraud to the Registrar. Cancel credit/GPC cards where unauthorised purchase has taken place and inform bank.
- c) Possible fraud detected by internal/external audit team should be reported directly to the Registrar. The Registrar will inform the police and keep DCMS and NAO updated.
- d) Review and strengthen controls immediately. Communicate any weakness and remedial action to relevant staff members.
- e) The Registrar in his capacity as Fraud Liaison Officer will ensure that an appropriate investigation is carried out and updates provided to DCMS, NAO and the PLR Audit Committee.
- f) Following the fraud PLR's Management Team will reassess the controls in place on the risk register to identify any weakness and implement improved controls.

6. Investigation of External Fraud

As the nature of fraud can vary considerably and each investigation may require its own unique approach to meet the circumstances which prevail, this plan does not set out to prescribe a detailed programme of action. For example, the police will wish to conduct their own investigation and it may not be necessary for the FLO to undertake a detailed separate investigation.

Managing the Investigation

- a) The Registrar will determine the objectives of the investigation and consult with DCMS where merited by the extent and severity of the fraud..
- b) The Registrar will determine the scope and timing of the investigation.
- c) The Registrar will approve the resources which will be available for the investigation.
- d) The Registrar should ensure that the resources used are monitored against the agreed budget.
- e) An investigation may not lead to criminal proceedings but may result in remedial action i.e. removal from the Register.
- f) The Registrar will provide a report to DCMS, NAO and the Audit Committee on the outcomes of the investigation.

Gathering and Securing Evidence

A diary of events must be maintained by the FLO; this should give a detailed explanation of each action and event in the course of the investigation. A successful criminal prosecution can depend on details, which in other contexts could appear unimportant. Also a considerable time could elapse between the start and conclusion of any investigation. Therefore, to aid recall all relevant details must be recorded in the diary of events. The following must be logged:-

- Details of all telephone calls, faxes, electronic mail and any other forms of communication.
- A clear record of where, when and how documents and other evidence were obtained.

FLO will take immediate charge of any original documentation that is relevant to the discovered fraud. These should be logged in such a way to identify the identification of the source, nature and purpose of each. If the alleged fraud involves the use of a computer, then the FLO should involve the IT Manager so that any records on a PC or network relating to the fraud cannot be accessed, destroyed or corrupted prior to the investigation.

Further Guidance

Managing the Risk of Fraud – A Guide for Managers (HMT May 2003)

NAO & HMT Guide: Good Practice in Tackling External Fraud 2008

Annual Analysis of Fraud in Government Departments

All above can be found on the Treasury website.

JANUARY 2012

