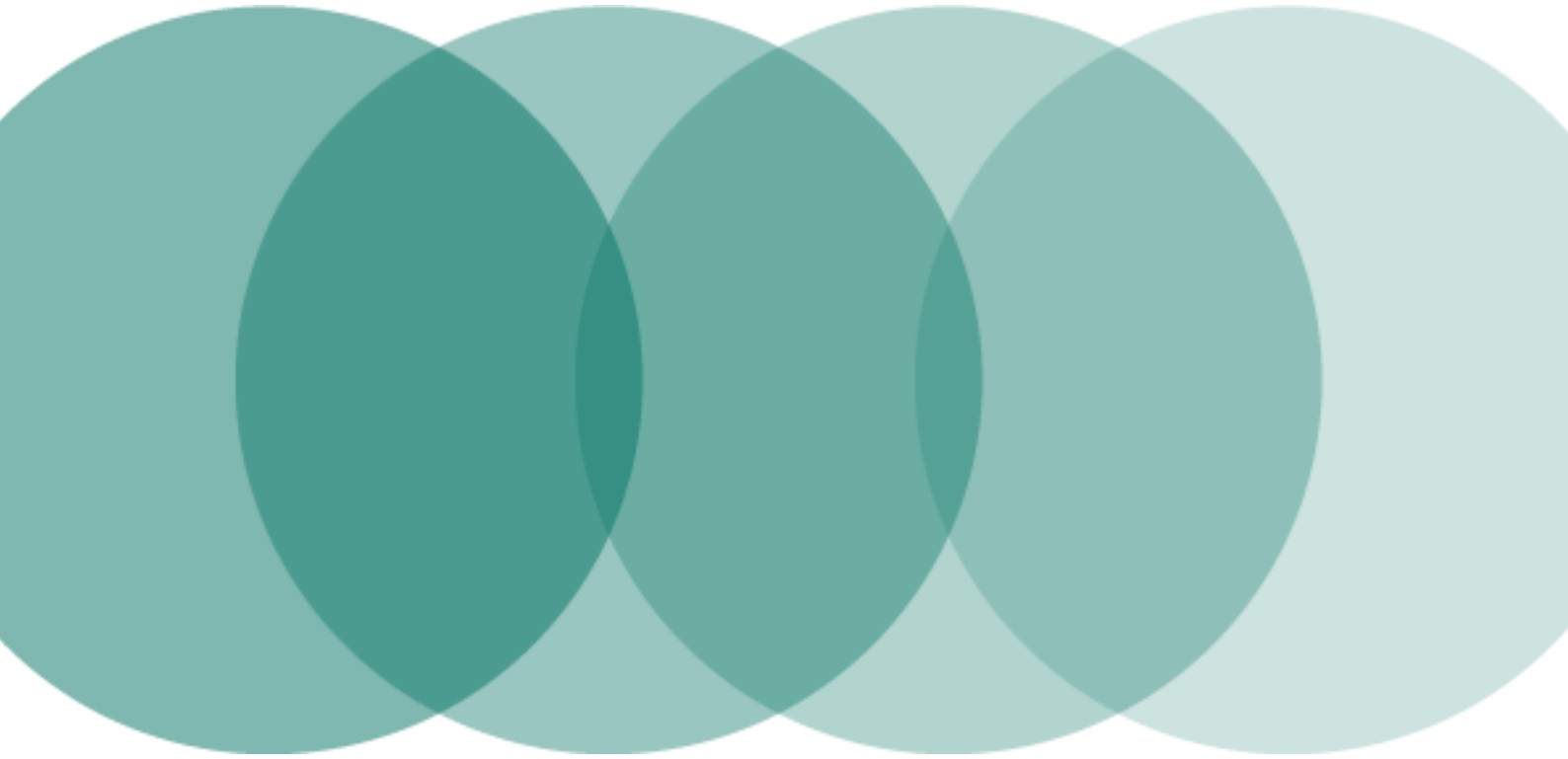
Ministry of Justice

Internal Audit and Assurance

Anti-Fraud and Corruption Policy



November 2014

Version 1.10

Contents

Introduction

What is Fraud

Management Responsibilities

Staff Responsibilities

MoJ Fraud Investigation and Prevention

Accounting Officers

Fraud Response Plans

Fraud Investigatuion and interface with Disciplinary Procedures

Recovery Action and lessons Learned

Bribery and Corruption

Whistleblowing' and Money Laundering

Review

Appendices

Examples of instance of fraud	A
Common fraud categories	B
MoJ Corporate Fraud response Plan	C

Executive Summary

1. The Ministry of Justice (MoJ) requires all staff to act honestly and with integrity at all times and to safeguard the public resources for which they are responsible. Fraud is a constant threat to the management of these resources and must be a concern to all members of staff.

2. The MoJ's policy on fraud and corruption is one of **zero tolerance**, whether involving its own staff, or other external individuals or bodies. It is MoJ's policy to refer all instances of fraud both actual and reasonably suspected to the relevant police authorities. All cases will be thoroughly investigated and dealt with appropriately. This policy statement sets out responsibilities with regard to the prevention, detection and reporting of fraud, and applies to all staff within the MoJ. Other executive agencies and NDPBs will have their own policies which are consistent with this policy.

3. This policy has been endorsed by the MoJ's Principal Accounting Officer (the Permanent Secretary) and the MoJ's Departmental Audit and Risk Committee.

What is Fraud

4. Fraud is a criminal offence. A general offence of fraud was created by the Fraud Act 2006. The three ways that fraud can be committed, as set out in the Act, are by:

    - False representation
    - Failure to disclose information when there is a legal duty to do so
    - Abuse of position

5. In each case (for example, through making a false representation) an individual must intend to make a gain for themselves or another, or to cause loss to another, or expose another to a risk of loss. The Fraud Act applies to offences committed in England, Wales and Northern Ireland, but does not extend to Scotland[1].

6. Offences such as theft, corruption, false accounting, forgery, counterfeiting and blackmail are separate offences enacted by other legislation. Further, there remains a common law offence of conspiracy to defraud.

7. In Scotland, fraud is a common law offence, best defined as the making of pretence by a person by which he obtains something he would not otherwise have obtained; related acts of bribery, forgery etc are separate common law offences distinct from fraud.

8. E-enabled / Cyber fraud is a generic term commonly employed when information technology has been used to manipulate programs or data dishonestly e.g. by altering, substituting, destroying records or creating spurious records or where the use of an IT system was a material factor in the perpetration of a fraud. This includes theft or fraudulent use of computer time and resources. Examples of instances of fraud are shown at appendix A.

[1] With one exception - Section 10 (1) re: the Companies Act 1985: Participating in fraudulent business carried on by a company

MoJ Fraud Investigation and Prevention

9. As part of the Ministry's commitment to fighting fraud, there are dedicated Fraud Investigation Teams for the LAA; HMCTS; NOMS and Core MOJ. These Teams are responsible for:

    - Promoting an anti-fraud culture
    - carrying out investigations into allegations of fraud
    - providing advice and guidance to management on how to deal with suspected fraud
    - unannounced visits to check on areas where there is a high risk of fraud
    - raising fraud awareness;
    - using investigation and analysis tools to interrogate corporate data to identify indicators of possible fraud;
    - Reporting to Boards and Audit Committees across the Ministry; and
    - Reporting through MoJ Internal Audit and Assurance to the Cabinet Office (Fraud, Error, Debt and Grants Team).

Accounting Officers

10. In accordance with HM Treasury guidance and the Cabinet Office Eliminating Public Sector Fraud, Accounting Officers should ensure that adequate arrangements have been established in their area of responsibility to identify and assess risk and maintain fraud risk assessments.

11. The MoJ Principal Accounting Officer and Accounting Officers' of subsidiary bodies are responsible for establishing and maintaining a sound system of internal control that supports the achievement of policies, aims and objectives for their areas of responsibility. Systems of internal control are designed to respond to, and manage the whole range of, risks that an organisation faces. They are based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively.

12. Accounting Officers should allocate overall responsibility for managing the risk of fraud in their area of responsibility to an appropriate senior officer. The senior officer's responsibilities will depend on the level of fraud risk to which the Accounting Officer's area of responsibility is exposed, but should include some or all of the following:

    - Developing a fraud risk profile and undertaking an annual review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current.
    - Establishing an effective fraud response plan, commensurate with the level of fraud risk identified in the fraud risk profile
    - Designing an effective control environment to prevent fraud commensurate with the fraud risk profile

    <u>Establishing appropriate mechanisms for:</u>

    - Reporting fraud risk issues
    - Reporting significant incidents of fraud (appendix B)

- Co-ordinating assurances about the effectiveness of anti-fraud policies to support the Governance Statement
- Making sure that all staff are aware of the MoJ's anti-fraud policy and know what their responsibilities are in relation to combating fraud

MANAGEMENT RESPONSIBILITIES

13. **All managers are responsible for:**

- The prevention and detection of fraud
- Assessing the risk of fraud through the overall assessment of business risk involved with the operations for which they are responsible.
- Ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively
- Regularly reviewing and testing the control systems for which they are responsible
- Ensuring that all allegations of fraud or theft are investigated. Where appropriate the Police must be informed. Action must be taken where fraud is proven.
- Where assets have been stolen, management must make every effort to recover them.
- Press Office (and Ministers) must be briefed where it is likely that a criminal case will be brought against an individual. Management must ensure that such action is taken.
- Managers should ensure that all contractors, agency and fee-paid staff are aware of this policy and are alert to the possibility of fraud and where to report instances of identified fraud.

STAFF RESPONSIBILITIES

14**. Every member of staff is responsible for**:

- Conducting themselves in accordance with the Civil Service Code, the Civil Service Management Code, MoJ Conduct and Disciplinary policies, which collectively require staff to act professionally and with integrity, objectivity, honesty, impartiality, to comply with the law and ensure the proper and efficient use of public money.
- Acting with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payment systems, receipts or dealing with suppliers
- Being alert to the possibility that unusual events or transactions could be indicators of fraud
- If an employee suspects fraudulent activity, extreme care must be taken not to alert the potential perpetrators of the fraud. The employee must make sure that s/he reports it immediately in line with instructions. On no account should they take any action to challenge staff that may be involved.

- All staff who suspect fraud or theft must report it either to their line manager or to the appropriate fraud investigation team listed below:

  Core MoJ / NOMS Fraud team on 0300 047 5200 or by email to; or
  xxxxxxxxxxxxxxx@xxxxxxx.xxx.xxx.xx or;
  LAA email - allegations@legalaid.gsi.gov.uk ; or
  HMCTS email - xxxxxxxxxxxxxx@xxxxx.xxx.xxx.xx or
  OPG on 0121 600 6153 or opgstaffinternalfraud@publicguardian.gsi.gov.uk

- Alternatively, you can refer to the MoJ Whistleblowing Policy reporting wrongdoing hotline (01527 544777).

- Co-operating fully with those conducting internal checks, reviews or fraud investigations.

Fraud Response Plans

15. **Managers must respond quickly in situations where fraud or theft is suspected or discovered by:**
    - having appropriate mechanisms in place;
    - identifying, managing and reporting fraud; and
    - ensuring sufficient counter fraud capacity to meet fraud risk and improving capability

16. Fraud response plans underpin the MoJ's fraud policy by providing detailed information on the promotion of an anti-fraud culture, the assessment of the risk of fraud, and the response in the event that an incident of fraud and suspected fraud is discovered.

17. All areas of the MoJ must have a fraud response plan which underpins the MoJ fraud policy.

18. Response plans should cover how fraud and attempted fraud should be dealt with. This includes details of what individual staff should do, how suspicions should be reported, how and by whom investigations will be conducted (including how investigation capacity and capability is maintained, and the interface with disciplinary process), and future fraud and corruption deterrence. A generic example of a fraud response plan is shown at appendix C.

19. Separate response plans should be maintained for each Accounting Officer's area of responsibility within MoJ and should include reference to relevant fraud reporting procedures.

Fraud Investigation and Interface with Disciplinary Procedures

20. If the outcome of a fraud investigation concludes that there is a reasonable suspicion of fraud having been committed, MoJ will put the matter in the hands of the police and a criminal prosecution may result. The matter may also be subject to disciplinary investigation, as advised by Human Resources. Disciplinary procedures include suspension pending the outcome of an investigation, disciplinary interview and post-hearing disciplinary action.

Recovery action and lessons learned

21. The MoJ will seek to recover losses in all cases where a fraud has been proven, either through court proceedings or by following internal disciplinary proceedings. Managers must ensure that, where a fraud has taken place, the risk surrounding the process or area affected is re-assessed. If changes are needed to reduce the risk of similar frauds occurring, the costs must be balanced against the benefits of the reduced risk.

Bribery and Corruption

22. It is an offence for a civil servant to corruptly accept any money, gift or consideration as an inducement or reward. Corruption can be defined as 'an act done with intent to give some advantage which is inconsistent with official duty and the rights of others'. It is the abuse of power by a public official for private gain and includes bribery and bias.

23. The Bribery Act introduced two general offences:

- Offering, promising or giving a bribe; and
- Requesting, agreeing to receive or accepting a bribe

24. Bribery is the offering, giving, receiving or soliciting of any item of value to influence the actions of an official or person in charge of a public or legal duty. There is also a specific offence of bribery of foreign public officials and a corporate offence of failure of commercial organisations to prevent bribery. To report suspicion or for advice on bribery and corruption contact:
Core MoJ / NOMS Fraud team on 0300 047 5200 or by email to
xxxxxxxxxxxxxx@xxxxxx.xxx.xxx.xx or;
LAA email on allegations@legalaid.gsi.gov.uk ; or
HMCTS email xxxxxxxxxxxxx@xxxxx.xxx.xxx.xx or
OPG on 0121 600 6153 or opgstaffinternalfraud@publicguardian.gsi.gov.uk

'Whistleblowing' and Money Laundering

25. All staff should be familiar with the confidential reporting procedure (Whistleblowing Policy) and relevant arrangements for reporting suspected instances of money laundering.

Review

26. This policy will be kept under regular review and any matters arising should in the first instance be referred to MoJ Internal Audit & Assurance.

Ministry of Justice
Date

APPENDIX A

Examples of Instances of Fraud

Theft – *defined as dishonestly appropriating property belonging to another with the intention of permanently depriving them of it*, for example theft of official cash or a colleague's personal belongings.

Corruption – *abuse of official position for personal advantage or gain*
e.g. staff who can self certify authorising false expenses claims.

Extortion – *to obtain money or favours by intimidation, violence or misuse of authority*
Using authority or information against a colleague to gain an advantage, e.g. a manager instructing a junior officer to place an order for goods/services with a specific supplier with whom the manager has a relationship.

Deception – *the act of deceiving someone*
Providing information that is untrue to gain benefit, e.g. giving false information about domestic circumstances in order to gain additional expense payments (for example, under public interest transfer conditions).

Concealment of Facts – *to cover and hide, to keep secret*
e.g. not informing pay section when a retired officer receiving a pension dies, with the result that payment is still made or not informing pay section when an overpayment has been made.

Misappropriation – *to take and use money dishonestly*
Stealing money for personal benefit and then replacing the original amount, e.g. borrowing from the cash box and replacing funds on pay day.

Forgery – *illegal copying, crime of making fraudulent imitation*
Falsifying authorising officers' signatures on documents for gain or to conceal other misdemeanours, e.g. authorising signature on invoices.

Embezzlement – *to steal (money) that belongs to the organisation one works for*
Stealing specifically from the organisation, e.g. computer equipment or petty cash.

Conspiracy– *a secret plan to carry out an illegal or harmful act*
e.g. several people all travelling on official business in one car but each making a T & S claim for travelling separately.

Collusion - *secret/illegal agreement or co-operation*
Agreement between a member of staff and a supplier to the financial benefit of both.

APPENDIX B

In accordance with Government Accounting Regulations the MoJ/NOMS must report all cases of actual or attempted fraud or theft. HM Treasury defines fraud and theft under various categories and, where internal investigations are conducted into allegations of fraud or theft then the following categories should be considered and used for the purpose of performing the investigation and reporting on the outcome and any disciplinary action and penalty awarded following a disciplinary hearing.

CATEGORY	EXAMPLES
Travelling, Subsistence and Personal Allowances Frauds involving travel and subsistence claims and personal allowances that require the completion of a claim for payment.	• Claims for journeys that were not made; • Claims for overnight subsistence but staying with relatives rent free; • Overstated claims; • Forged signatures on claim forms; • Claims for allowances for which there was no entitlement; • Claims relating to circumstances no longer applying such as excess fares, lodging allowances; • Forged receipts (e.g. fuel bills, hotel bills, taxi receipts).
Pay or Allowances Paid via the Payroll Fraud involving payment via the payroll process.	• The creation of “ghosts”, “echoes” and other fictitious employees on the payroll; • False claims such as overtime and other taxable allowances; • Altered performance markings or false documentation leading to bonus payments; • Unauthorised changes to payroll data; • Deliberate failure to repay advances of salary; • The retention of credits, supplements or allowances beyond the period of entitlement; • Misuse of pay advances or loans (e.g. season ticket advance used for purposes other than the purchase of a season ticket to the value of the advance).
Theft of Physical Assets or Cash Thefts of cash or physical assets.	• Theft of cash (e.g. Cashier, Reception petty cash floats); • Theft of physical assets (e.g. items recorded on the local asset register or the fixed asset register).

Exploitation of Assets and Information This type of fraud involves using assets of the organisation for other than official purposes and/or supplying information to outside organisations for personal gain. NB: cases of unauthorised access to information without a fraudulent intent should be excluded.	• Using official vehicles for personal gain; • Running own business using the organisations assets (e.g. IT system); • Selling information to mail shot companies; • Downloading pornography for sale.
Procurement Fraud Procurement is the whole process of acquisition from third parties and covers goods, services and construction projects.	• Manipulating tenders/collusive tendering (including rings and cartels); • Rigging specifications in favour of one supplier; • Product substitution or sub-standard work or service not meeting contract specifications; • Theft of new assets before delivery to end user and before being recorded in the asset register; • Fraudulent (false or duplicate) invoicing for goods or services not supplied or for interim payments in advance of entitlement; • Improper or unauthorised use of Government furnished equipment or information; • False accounting and cost misallocation or cost migration between contracts; • Goods ordered for personal use; • Provision of fraudulent test or quality assurance certificates; • Corruption or attempted corruption of Crown Servants.
Grant Payments Grants to third parties the fraud risks associated with payment of grants include	• Unauthorised use of Grant funds which are misappropriated • Fraudulent applications
GPC/Credit Card Fraud All cases involving the improper use of GPC or credit cards.	• Covers the use of the Government Procurement Card.
Personnel Management Related Fraud Cases reported under this category should only include those where the action taken against the perpetrator involves some personal disadvantage or deprivation. Where oral or written warnings have **only** been issued cases should **not** be reported.	• Staff on sick leave but working elsewhere; • Serious abuses of flexible working time system; • Annual leave abuses; • Misuse of official time (e.g. Internet abuse, playing electronic games, abusing the department's computer misuse policy, sleeping whilst on duty); • Deceit and misrepresentation for advantage (e.g. false references or false qualifications

	used to secure employment.
Payment Fraud Theses are frauds which involve expenditure systems relating to payments for resources acquired for official use and consumption. Payments involving claims by an employee will normally be covered under “travel, subsistence and allowances” or “pay related frauds”.	• Creating false payments; • Theft of completed payable orders; • Theft of letters containing payable orders prior to posting; • Providing confidential information to outsiders allowing them to make fraudulent claims; • False accounting; • Theft of cash (i.e. petty cash floats used for making small payments); • Creating false BACS payments (e.g. adding records to a BACS file before it is sent to the bank).
Fraud Relating to Departmental Income This type of fraud covers theft of income.	• Theft of income (e.g. income received that has not yet been recorded in the accounting system such as income received by post, cash or cheques awaiting banking); • Understating or failing to record income so that “surplus” income can be stolen (i.e. false accounting); • Manipulation of fees/charges/sales records; • Manipulation of debtors records and write-off provisions; • Theft of income received via the post/Reception after it has been recorded in the accounting system.
Other Fraud and theft not falling into the above categories.	• Counterfeit/forged bank notes.

APPENDIX C

MoJ Corporate: Fraud Response Plan

This fraud response plan is one of a series which supports the MoJ's Anti-Fraud and Corruption policy; it sets out what you should do and how MoJ will respond in the event a fraud is discovered or if there is suspicion of a fraud in MoJ. Separate Fraud Response Plans will be established for each Accounting Officer's area of responsibility.

This plan specifically relates to the following business groups

- Finance Assurance & Commercial Group,
- Law & Access to Justice Group,
- Criminal Justice Group,
- Legal Aid Agency (LAA) & Corporate Services, and
- any other business area within the Ministry not covered by one of the other Fraud Response Plans in this series.

The plan covers procedures for how suspicions should be reported and how, and by whom investigations will be conducted. The details of the plan below will apply whether it is an internal or external fraud:

- Internal fraud (i.e. involving staff within MoJ)
- External fraud (people outside MoJ committing fraud against it)

Media and publicity

As a high profile public Ministry administering justice, it is possible that fraud committed internally or externally will be of interest to the media. Heads of Divisions (or equivalent) will be responsible for briefing the Press Office and all media enquiries should be referred direct to the Press Office.

Reporting the fraud or suspicion

At the point where a fraud, or a suspicion of fraud, is discovered the member of staff concerned must immediately report the matter to their line manager who will inform their Head of Division or equivalent (see also whistle blowing policy). If there are difficulties with this course of action, the individual should report the matter directly to their respective team for HMCTS email investigations@hmcts.gsi.gov.uk; for Legal Aid Agency on allegations@legalaid.gsi.gov.uk and for all other departments to MoJ Internal Audit & Assurance on the fraud hotline 0300 047 5200.

The following action must then be taken:

- The Head of Division or equivalent must notify the appropriate MoJ specialist fraud team, Finance and Human Resources.
- the appropriate MoJ specialist fraud team will provide timely advice on investigation action, including contact with the police.
- The Head of Division (or equivalent) should ensure their Director (or equivalent) is notified and updated about ongoing actions.

It is essential that members of staff and their managers respond quickly in situations where fraud is suspected or discovered. The individual or individuals under suspicion should not be alerted to the fact until the Head of Division (or equivalent) has contacted and obtained guidance from the appropriate specialist fraud team

.

External service providers - (e.g. Liberata, Capita, Atos Origin etc) on discovering fraud or suspicion of fraud should contact their MoJ contract manager and MoJ Internal Audit & Assurance.

Investigation

The Ministry maintains teams of specialist staff available to undertake fraud investigations. All investigations undertaken in England and Wales will comply with best practice guidelines under the Police and Criminal Evidence Act 1984 (PACE) and the Criminal Procedure and Investigation Act 1996 (CPIA). All investigations in Scotland will be undertaken in accordance with the Scottish common law principle of fairness toward an accused. Formal interviews will be tape-recorded and may be conducted under caution.

Investigators have been trained in interviewing and investigating and managers must not attempt to undertake any investigations or interviews themselves, as this may prejudice any future prosecution and/or disciplinary action. If a manager has any concerns that an irregularity has taken place they should contact MoJ Internal Audit & Assurance for advice before taking any action themselves. The individual under suspicion must not under any circumstances be spoken to about the suspicion or allegation of fraud. However, if an individual wishes to make an immediate statement, you may accept it but ensure that:

- the statement is in writing
- it is taken immediately, or as soon as possible after the event

- no questions are asked of the individual
- notes are made, then signed and dated by all in attendance
- notes and statements are retained securely, and where circumstances allow:
- the statement is given in the presence of yourself and another manager independent of the allegation
- a Trade Union representative, workplace support (welfare) representative, or colleague is available to support the individual.

In the case of external frauds against the Ministry, the police will conduct the investigation with assistance from Ministry investigators /internal audit, as appropriate.

Securing evidence

At the point where a fraud or a suspicion of fraud is discovered, all evidence material to the investigation must be secured. Line management may be asked to collect the appropriate documents and to ensure secure storage until the members of an investigation team can take formal custody of the documents. (This may mean various types of financial record, attendance sheets, receipt books, files etc).

It is extremely important that the handling of any evidence is kept to an absolute minimum and that all evidence is secured immediately. It is advocated that cheques, payable orders and other documentary evidence are placed in transparent wallets, in order that they can be viewed without destroying possible fingerprint evidence. Bulkier items should be placed in folders or boxes.

If asked to collect and secure the appropriate documentation, staff and managers must not make any markings or endorsements nor tamper with the documents in any way, to prevent possible prejudice of any future prosecution. Items must be secured as quickly as possible to prevent any accidental loss or destruction of the evidence.

If computer records are to be used in evidence as part of an investigation, the hardware and data storage media must be placed under secure safekeeping until a qualified investigator can attend. Access to systems and data on any system that it is suspected has been used to commit fraud must be prohibited to individuals under suspicion.

Desk searches

Where it is necessary to search desks, pedestals lockers etc, it will normally be carried out by two investigators in the presence of the member of staff concerned, a manager and a trade union (TU) representative, provided this does not delay the investigation. Exceptionally, where it is not possible to include the individual concerned (e.g. the individual is suspended from duty or

off sick) the search will be carried out in the presence of witnesses, who can be the individual's line manager, business manager and a TU representative, provided this does not delay the investigation unnecessarily.

Police action

The police will be contacted in all cases where there is a clear indication of a fraud having been committed. MoJ Internal Audit & Assurance will advise on whether the police should be contacted.

Employees under suspicion

In the event that an employee is under suspicion the options detailed below are available to you when the immediate action of the investigation process has been complied with.

Line management should consult with the head of division (or equivalent) to determine whether it is appropriate to send the individual home. The head of division (or equivalent) should contact MoJ Internal Audit & Assurance at this stage before any decision is made to send the individual home.

Sending an individual home can be done for up to two days without it being considered a suspension. This course of action does not imply guilt, but is a measure aimed at protecting both the individual and the Ministry while initial enquiries are made. The individual should be informed of the allegation, but it is essential that no accusation is made against them. The individual should be invited to consult with a trade union representative, a member of workplace support (welfare) or a colleague for support. Managers must ensure that all proceedings are conducted without prejudice and in strictest confidence.

If an individual is sent home, the manager or an independent manager must accompany the individual to their desk so that all personal belongings, but only personal belongings, can be removed. (See desk searches). The manager must also seek the return of all official equipment and documentation, including security passes, Government Procurement Cards, laptops, mobile devices or money held by the individual at home or in an official vehicle. If the individual is an official car user the senior manager should seek the return of the overdrive card, but should not take possession of an official vehicle unless asked to do so. The individual should then be escorted from the premises. It may also be appropriate to change door codes and to change passwords on computers, as well as securing them.

Human Resources should be informed immediately and they will advise on the appropriate action to be taken, including the decision on whether to invoke formal suspension. The head of division (or equivalent) must authorise formal suspension.

Disciplinary action

If the outcome of a fraud investigation identifies the perpetrator of a fraud, the Ministry will refer the matter to the police for possible criminal prosecution.

At the same time, the matter will need to be investigated in accordance with the Ministry's disciplinary procedures. The head of division (or equivalent), as advised by Human Resources, will take decisions concerning disciplinary action. These procedures include suspension pending the outcome of an investigation, disciplinary interview and post-hearing disciplinary action. If failures in management control have contributed to the opportunity for fraud, then disciplinary action may also be considered against those officers concerned.

Recovery action

The Ministry will seek recovery of losses in all cases where a fraud has been proven, either through court proceedings or following internal disciplinary proceedings. Where court proceedings are being brought, managers should ensure details are supplied in order for a claim for compensation to be sought. Where an employee is dismissed, managers should ensure that a claim for the loss is off set against any monies due to the employee.

Dissemination of lessons learned

Managers must ensure that where a fraud has taken place the area of risk is re-assessed. If appropriate, changes should be made to ensure that the risk of similar frauds occurring is balanced against other factors, such as the cost of increased control.

MoJ Internal Audit & Assurance monitors details of all frauds and where appropriate, summary details of the fraud will be circulated across the Ministry to key staff, so that lessons can be learned and procedures reviewed. The employee in question will remain anonymous.

Fraud Awareness

Training in fraud awareness is an essential part of the induction material and events provided for all new members of staff. Awareness of Managers' responsibilities in relation to disciplinary and conduct issues, including suspected fraud, is covered in 'Laying the Foundation courses'.

Whistle blowing

The Ministry has established a whistleblowing (or confidential reporting) policy, which allows any member of staff with a serious concern about any aspect of the work within the Ministry, to report their concerns through a confidential reporting procedure. The policy takes into account the requirements of the Public Interest Disclosure Act 1998.

This policy applies to all employees, and those contractors working for the Ministry, for example, agency staff, builders, security, or catering staff. It also covers suppliers and those providing services under a contract with the Ministry in their own premises. Within the policy the phrase "employees" includes all the above.

Members of staff should use this policy if they believe they are being required to act in a way that is inconsistent with the Civil Service Code. However, this policy also includes other areas of serious concern, such as the unauthorised use of public funds, fraud and corruption. The full Whistleblowing policy is available on the MoJ Intranet.