Appendix A

Nottingham City Council

Fraud Response Plan

Nottingham City Council October 2011, updated November 2015 and November 2017

Contents

Appendices

1 Introduction and Objective

Nottingham City Council is committed to protecting public funds. Minimising the losses to fraud and corruption is an essential part of ensuring that all of our resources are used for the purpose for which they are intended - the provision of high quality services to citizens. We have a range of policies and procedures that facilitate the 'zero tolerance' approach adopted. These include the:

- The City Council constitution
- Accounting procedures
- Financial regulations and Standing Orders
- Colleague Code of Conduct
- Fraud Awareness Training
- Counter Fraud Strategy
- Prosecution Policies
- Confidential Reporting (Whistleblowing) Policy

The public is entitled to expect the City Council to conduct its affairs with integrity, accountability, honesty and openness, and demand the highest standards of conduct from those working for it and with it. Therefore one of the Council's main objectives, to combat fraud and corruption, is to identify and maintain good practices, address weaknesses in current processes and introduce improved systems for the management of those processes. This will ensure that the potential for fraud is kept to an absolute minimum. It applies to all Councillors and all personnel whether direct employees of Nottingham City Council, agency staff or contractors.

NCC Financial Regulations require that matters involving any suspected financial irregularities are referred to the Head of Internal Audit. The decision as to whether or not the irregularity should be investigated will be taken at his direction. All referrals are taken seriously and the action to be taken guided by an assessment of the risk. Where fraud is found, appropriate criminal investigation, disciplinary action and police involvement will be pursued. Losses will be recovered wherever possible and incidents of successful prosecution publicised.

Management and colleagues are likely to have little experience in dealing with fraud and, when suspected cases arise, may be unsure of the appropriate action to take. This document is intended to provide direction and help to colleagues in dealing with suspected cases of theft, fraud and corruption. It also gives direction to others wanting to report matters of concern.

The objective is to safeguard the proper use of the City Council's finances and resources.

2 Reporting fraud suspicions

2.1 Initial guidance if you suspect a fraud.

A fraud may be uncovered in a variety of ways, from your own observations, someone from inside or outside blowing the whistle, ongoing controls throwing up a discrepancy, internal or external audit discovering a problem, or external regulators and inspectors finding something. It is important for you to know how to deal with your suspicions.

Things to Note

- Stay calm – remember you are a witness not a complainant. Write down your concerns immediately – make a note of all relevant details such as what was said in phone or other conversations, the date, the time, the names and contact details of anyone involved. Consider the possible risks and outcomes of any action you take Make sure your suspicion is supported by facts, don't just allege.

- Do not become a private detective and personally conduct an investigation or interviews. Do not approach the person involved (this may lead to him/her destroying evidence). Do not discuss your suspicions or case facts with anyone other than those persons referred to below unless specifically asked to do so by them. Do not use the process to pursue a personal grievance.

- You may be mistaken or there may be an innocent or good explanation – this will come out in the investigation. The process may be complex and you may not be thanked immediately and the situation may lead to a period of disquiet or distrust in the organisation despite your having acted in good faith.

- Where there is clear evidence of a theft of physical assets or cash, the police should be notified immediately.

2.2 Reporting your suspicions

The following reporting lines are to be used regardless of the potential magnitude of the fraud, which it would be difficult to quantify at an early stage. 2.4 overleaf illustrates the thought processes to be considered in determining the most appropriate reporting route. The following points may be useful

- **Your line manager**
  Generally this is your first port of call. Fraud prevention is their responsibility in particular. They will know the systems, the people, what is at risk. They should know whom to bring in.

- **A more senior manager or your Director**
  If you think your manager might be involved in the fraud or if you feel they have wrongly dismissed your concerns, then you should go to a more senior manager or your Director.

- **Fraud reporting email / internet**
  If you do not wish to make the report directly to your line manager the Council has in place electronic methods of reporting your concerns. If you want to be assured of absolute confidentiality or wish to remain anonymous, you can report to the Head of Internal Audit or his Corporate Counter Fraud Team. You may do this directly or by using fraud@nottinghamcity.gov.uk, or the reporting buttons available on the Council's websites.

- **Whistleblowing**
  The Whistleblowing Policy on the intranet provides advice on reporting criminal acts (such as fraud). You should acquaint yourself with this policy before deciding to report the incident under the policy or as a fraud. If you wish to make a report under this policy you should contact the appropriate person identified in the policy who will then liaise with the Monitoring Officer or Head of Internal Audit. You may of course access the Monitoring Officer or the Head of Internal Audit direct or use the appropriate electronic mechanism on the Council's websites. Provided reports are made in good faith, you are protected by the Council and the law against retribution, harassment or victimisation and your confidentiality will be preserved.

  If you feel unable to use Council's procedure for your disclosure you can contact an independent "prescribed" person who can also provide you with the appropriate employment protection, rights. If you make a disclosure to a prescribed person it is escalated outside the Council, since those with investigatory and regulatory functions can act upon the information provided, if they consider it necessary.

2.3 Guidance for line managers on receiving a report of fraud:

- Listen to the concerns of your colleagues and treat every report you receive seriously and sensitively. Make sure that all colleagues concerned are given a fair hearing.

- You should reassure your colleagues that they will not suffer because they have told you of their suspicions.

- Obtain as much information as possible from the colleague. Do not interfere with any evidence and make sure it is kept in a safe place.

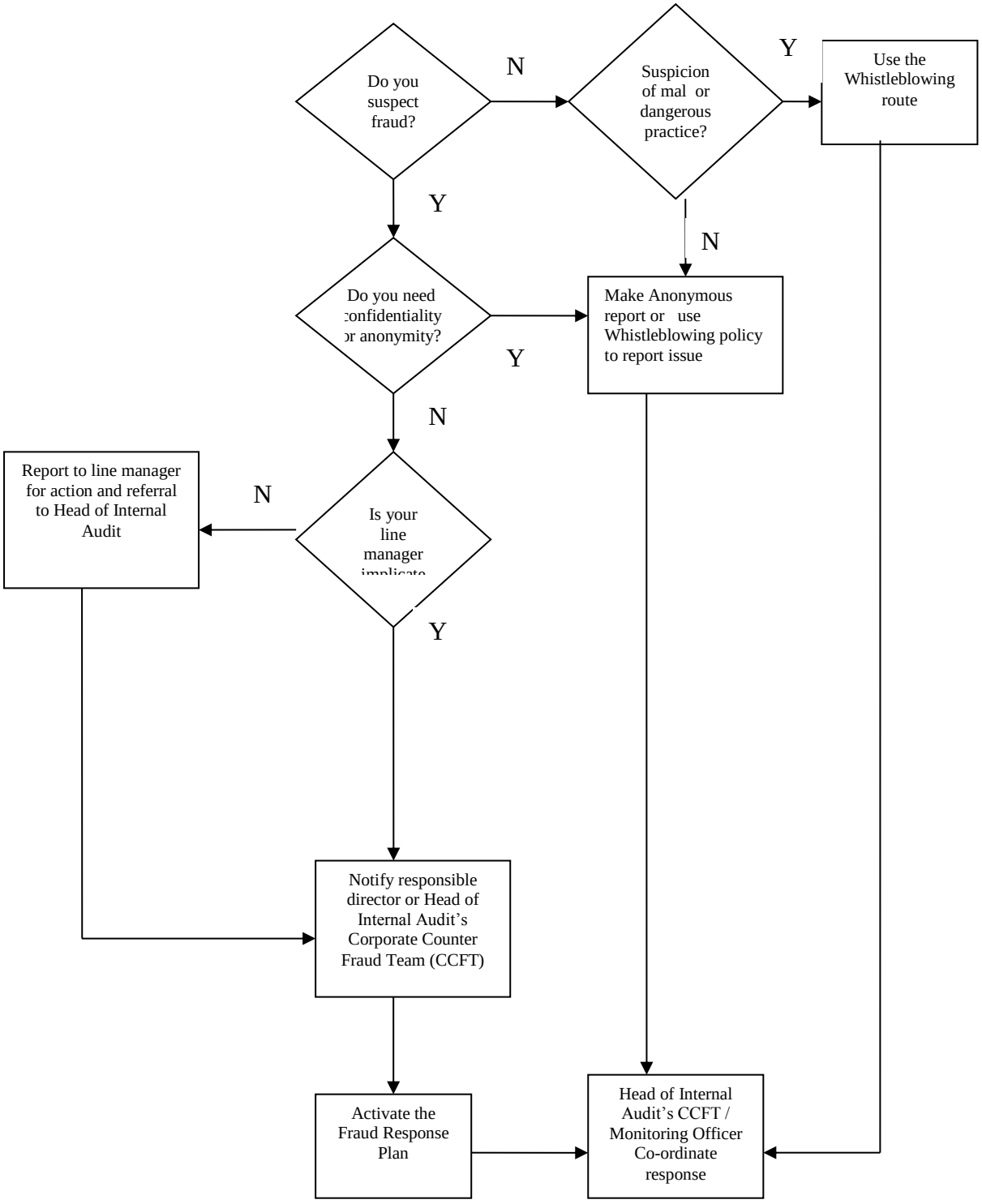
- Request the colleague to keep the matter fully confidential in order that senior management are given time to investigate the matter without alerting the suspected/alleged perpetrator.

- Report the matter immediately to the Head of Internal Audit who will arrange a full investigation of the matter and ensure an appropriate response is made.

2.4 Decision Tree and Actions

Identified a Potential Fraud or Whistleblowing issue?

Refer to Financial Regulations and Whistleblowing Policy



3 Fraud Response Plan

3.1 Introduction

It is important that managers and others know what to do in the event of a fraud so that they can act without delay. The Fraud Response Plan covers the action required when fraud is suspected and to whom the fraud or suspicion should be reported. The Fraud Response Plan is a guide to how and by whom the fraud suspicion will then be investigated, reported and closed.

The Fraud Response Plan provides an outline of many of the areas that will need to be considered when investigating a large and complex fraud. For smaller less complex frauds, there will be parts of the plan that will not be applicable. It is however important to keep an open mind and consider whether a small fraud is concealing a much larger fraud.

3.2 Immediate Action

All cases must be notified to the Head of Internal Audit and may also be reported to the Director or Line Manager

The Head of Internal Audit will ensure that all suspected fraud is recorded in the Fraud / Whistleblowing Register and updated as the investigation progresses (see appendix 5).

3.3 Head of Internal Audit - Fraud Response

The Head of Internal Audit will arrange for the most appropriate response, including the provision of investigative resources from the department and where required from the Corporate Counter Fraud Team (CCFT) and the Legal Service. For small or less complex frauds, a large investigative resource may not be required, but the Head of Internal Audit should always be kept informed of progress at all stages of the investigation.

- Investigative Resources should be established as part of agreeing and signing off the Fraud Response Plan.
- Investigators should quickly determine the following:
    - whether an investigation is necessary
    - who will lead the investigation (the person chosen to lead the investigation should be appropriately experienced and independent of the activity affected by the alleged fraud).
    - any necessary additional resource to support the investigation
    - any immediate need for police involvement
    - any additional support requirements (eg IT facilities, a secure room, secure fax and phone facilities, administrative support etc)
    - any immediate need for legal advice
    - any immediate need for external, technical advice or support (eg forensics)
    - any immediate need to establish a PR/media strategy for dealing with the case (both internally and externally)
    - any immediate need to suspend colleagues; conduct searches and remove access (eg to files, buildings, computers/systems etc)
    - any immediate need to report the potential fraud externally (eg external auditors, tax authorities etc)
    - whether insurers need to be informed

- whether the chair of the Audit Committee should be informed
- a timetable for the lead investigator to report back progress on the investigation.

- The objectives of the investigation should be documented and approved by the Head of Internal Audit at the outset. Likely objectives would be to:
  - establish if a fraud has taken place
  - identify the culprit(s)
  - establish the facts surrounding the fraud and ascertain total losses
  - remove the threat of further losses. (Note: in some exceptional cases it may be necessary to allow further losses, in order to gain additional evidence and increase the chances of successful criminal, civil, or disciplinary action. This should normally only be allowed under police guidance).
  - obtain sufficient evidence for successful disciplinary, criminal, or civil action
  - Certain action may need to take place immediately to prevent further losses.

- The Director/Head of Human Resources should be involved on any decisions and action regarding suspensions and removal of access to files, systems and offices.

- The date of the next meeting and review of the first investigation progress report should be agreed.

- The Head of Internal Audit should be updated on a regular basis, to oversee progress of the investigation and to take major decisions relating to the case.

3.4 The Lead Investigator's Plan

- The lead investigator should prepare an investigation plan, which should be submitted to the Head of Internal Audit for approval.

- The Plan should be fairly short term, as developments in the investigation will invariably result in changes. It should clearly show what work/tasks need to be completed, why they are necessary, by whom and by when.

- The Plan may cover some or all of the following:
  - identification and recording of the persons involved and facts of the case
  - handling internal and external communications
  - actions to prevent further losses
  - actions to secure evidence. Normally, evidence should be secured in a way that will be least likely to alert the suspect(s) or others
  - liaison with Human Resources and dealing with colleagues under suspicion
  - interviews to be conducted
  - timetables for involving the police or other external experts
  - analysis of evidence
  - internal reporting (eg to Management Team, Audit Committee, etc)
  - reporting to regulatory/government bodies and or the Police
  - target dates for reporting back to the Head of Internal Audit

3.5 Communications during and after the investigation

The effectiveness of the Plan depends on good quality communication at all stages.

Internal communications

- Investigators need to ensure that everyone with a need to know is kept suitably briefed throughout the investigation and at the reporting, acting on findings and debriefing stages. Communication with any person(s) about whom concerns are raised needs to be conducted in accordance with the Council's HR policies. The person who raised concerns should be kept up to date, with due regard to confidentiality.

- There will always be a balance to be struck between communication and confidentiality therefore those persons or categories of persons who need to know should be clearly identified at each stage of the Plan, so that assurances on confidentiality can be given where required

External communications

- Third parties who may need to be alerted or informed might include the Police, regulatory authorities, insurers, legal advisors and external auditors. The Plan should make clear who is mandated to communicate with these third parties, and under what circumstances.

- The Council is prepared for the fact that frauds may attract media attention and the Plan should identify which colleague is mandated to deal with the press and what action any other colleagues contacted by the press should take. The current media communication channels and procedures should be used where possible

Inappropriate communication

The Plan should make clear any form of communication that is considered inappropriate, for example:

- discussing the case outside the Council
- confrontation between the person reporting the fraud and the suspected perpetrator(s). (Note that the Whistleblowing Policy provides assurances for the safety and confidentiality of the person making the report.)

3.6 Securing evidence

- In securing and handling evidence it should be assumed that all evidence may need to be examined forensically and presented in court and should therefore be treated accordingly. (Even if criminal or civil action is not planned, it is sensible to adopt this approach.)

- Normally, all evidence should be kept securely under lock and key, with access limited to those working on the investigation. If necessary, locks to secure rooms should be changed. Evidence should be handled appropriately and a record should be maintained of anyone handling it.
- Evidence such as computer data, transferable media, videotape etc, should only be handled by suitably trained and skilled personnel. Where there is any doubt, professional/Police advice should be sought.

- Where evidence, or other relevant information, is to be shared with another body, careful consideration should be given to any data protection (confidentiality) requirements. Where there is any doubt, expert advice should be sought from the Council's Legal Services or Information Governance team.

- Evidence can take different forms and will need to be handled in different ways, for example:

  Original Documents
  - handle as little as possible
  - put in protective folder and label the folder
  - do not mark in any way
  - assign responsibility to one person for keeping the documents
  - keep a clear record of how and where the documents were obtained
  - keep a record of anyone who subsequently handles the documents

  Computer Held Data/Transferable Media
  - keep secured in an appropriate environment
  - data should only be retrieved from computers by those who are technically qualified

  Photocopied Documents
  - in some cases it may be preferable or necessary to leave original documents in situ and take photocopies for further analysis and investigation
  - photocopies should be clearly marked as such
  - photocopies should be signed and dated, and certified as a true copy of the original

  Other physical evidence (including Video/DVD/CD Rom)
  - keep secured in an appropriate environment (eg protective bag)
  - videos should not be viewed until technical and legal advice is sought in order that they can be treated in accordance with the rules of evidence

  External evidence
  - There are potential external sources from which evidence or information to support an investigation can be obtained, such as the tax authorities, supplier records, government registers of companies, donor records etc.

3.7 Colleagues under suspicion

- It should always be remembered that an allegation of fraud may be unfounded and in order to respect the colleague and ensure good working relations after an investigation, any action taken, such as suspension, and interviewing should be handled very carefully.

- Suspension from work is an opportunity to protect both the employer and colleague, providing the necessary space and opportunity to plan the investigation, investigate the facts and speak to other colleagues without the colleague being present. It should be made clear that suspension is not a judgement.

- The key factors in deciding to suspend colleagues will normally be prevention of further losses and removal or destruction of evidence. In some cases, it may be preferable to not suspend even at the risk of further losses (eg to gather further evidence).

- Any colleagues under suspicion who are allowed to remain at work should be closely monitored. This may include: physical surveillance of movements, monitoring of IT usage, monitoring of telephone, email and internet usage etc. (Note: it is advisable to seek legal advice regarding the use of surveillance techniques, to ensure compliance with local laws such as the Regulation of Investigatory Powers Act in the UK).

- Where a suspect offers to resign during the investigative process the consequences must be considered and a decision to reject or accept the resignation made only after consultation with HR, Legal Services and the Head of Internal Audit. By accepting the resignation the Council's ability to investigate the incident and gain proper redress may be limited.

- Other matters to consider include:
  - A review of HR records (eg to check references, employment history, qualifications etc, but with due regard to any data confidentiality / protection requirements)
  - Searching the suspect's work area; desk, cabinets, files, computer etc
  - Restricting access by the suspect to files, computers etc.

3.8 Interviews/statements

- When interviewing colleagues under suspicion it must be made clear whether it is a formal interview or an informal discussion. It should be explained that you have no pre-set view, the suspicion should be outlined and the colleague given adequate time to respond.

- If it is decided that formal questioning is needed because involvement in a criminal offence is suspected, then the CCFT should be consulted to consider whether the interview should be conducted in accordance with the principles of the UK Police and Criminal Evidence Act (PACE). Guidelines can be found on the Home Office Website.

- Interviews should only be carried out with the approval of senior management/the Head of Internal Audit.

- Early consideration should be given to Police involvement, or consultation.

- There are strict rules relating to tape recorded interviews and investigators must be suitably skilled and experienced, where these are used.

- Ideally, statements should be taken from witnesses using their own words. The witness must be happy to sign the resulting document as a true record – the witness can be given a copy of the statement if desired.

- It is very important to keep contemporaneous notes on file, in the event that they are needed for future reference (e.g. court, tribunal, disciplinary hearing). Such notes

should always show: date of interview; time started; time finished; and be signed and dated by the interviewer.

3.9 Police involvement

- Discussions should take place with the Head of Internal Audit regarding the best course of action in each case. A decision will need to be made as to whether the case is reported to the Police but other alternatives should be considered, for example a private prosecution. For large-scale / serious frauds, it may be appropriate to inform the Chief Executive and ask the Police to attend meetings with the investigators, Head of Internal Audit and legal advisors.

- Where a decision is taken to pass the matter to the police, the lead investigator should prepare an evidence pack that can be handed to the police at the time the fraud is reported. The pack should include a summary of the fraud, highlighting (where known) the amount, the modus operandi, and the location, and including photocopies of key supporting documents and contact details of the person leading the investigation.

- Where practical a record of everything that is handed to the Police should be kept

- All contact with the police should be channelled through one person (ie the person leading the investigation). A record should be maintained of all contacts with the Police, the details of the officers, and the crime reference number.

- The Police have knowledge of similar cases of fraud and their advice should be sought regarding measures to prevent further losses or future incidents.

3.10 Prevention of Further Losses

- Once actual or potential losses have been identified it is important that effective and timely action is taken to prevent further losses. It may however be decided that a better standard of evidence can be obtained by allowing limited further losses.

- The person in charge of the investigation should, at an early stage in the process, complete a preliminary assessment of the potential for further losses and how best to prevent them. He should make recommendations to senior management as to what if any immediate actions are necessary.

- Actions taken at an early stage may have to be circumspect so as not to alert suspects who have yet to be suspended or cautioned. It may also be important not to lose or compromise the forensic value of data by precipitate action. It may nevertheless be necessary to act quickly e.g. to stop payments to suspects who are being investigated.
- As the investigation continues, and more information emerges, further recommendations for action may be needed. At the end of the investigation, Internal Audit should review all the actions taken to prevent further losses and to report on this in the Review of Findings.

3.11 Recovery of Losses

Once the identity of the perpetrator(s) and the size of the fraud has been determined, management must consider whether or not any of the loss can be recovered and take any further action that is necessary. This may require advice from the Insurers.

Reimbursement offered during the investigation

- An individual may, in the course of an investigation, offer to repay the amount that has been obtained improperly. The person in charge of the investigation should neither solicit nor accept such an offer (as it may be construed as having been obtained under duress). The lead investigator should record any offer made and refer the individual to the Head of Internal Audit who in turn will consult with the Chief Finance Officer and Director of Human Resources.

Reimbursement offered during disciplinary or legal proceedings

- If an offer of restitution is made while disciplinary or legal proceedings are still under way, management must seek legal advice before such an offer is accepted.

Reimbursement after completion of disciplinary proceedings

- Where a colleague is to be dismissed, the manager should consider recovery of amounts due from any outstanding salary or expense payments. It will be necessary to take legal advice about the right to do this, as it is unlikely to be clear in the colleague's contract of employment.

Recovery of loss

- Where the Council has suffered loss, restitution will be sought of any benefit or advantage obtained and the recovery of costs will be sought from individual(s) or organisations responsible for fraud.

- Where a colleague is a member of Nottinghamshire County Council's Pension scheme, and is convicted of fraud, NCC may be able to recover the loss from the capital value of the individual's accrued benefits in the Scheme, which are then reduced as advised by the actuary.

Court Order

- Where a criminal case is taken against an individual a formal claim for restitution (where the court orders the defendant to give up gains) or alternatively a compensation claim made within a proceeds of crime claim should be made through the Police. Seek advice from Legal to determine the appropriate claim. Any monies due will be recovered via a Court Order.

Civil Action

- Funds lost due to fraud can be recovered from the perpetrator by suing them for damages in a civil court. The level of proof required in civil cases is lower than that required in criminal cases and management may regard a civil action as a more effective use of their time than trying to persuade the Police to investigate and the courts to prosecute. If this approach is successful, the perpetrator will also have to pay the Council's legal costs. Seek advice from Legal to determine the appropriateness of the claim.

- A civil action can still be brought even if a criminal prosecution has failed. If a criminal prosecution is successful a civil action may be necessary to force the person convicted to repay the sums stolen.

- It is important to remember that the person being sued may be unable to make the repayment. In situations in which repayment is unlikely senior management approval should be obtained before additional legal costs are incurred.

Commercial Negotiation

- Where the fraud has been committed by the employee of a contractor or supplier, all or part of the loss may be recoverable from the business concerned. It may be possible to reach an agreement that the loss can be deducted from any outstanding debts or that additional goods/services will be supplied free of charge.

- Third parties may want to agree a negotiated settlement in order to retain the goodwill of their customer and/or to avoid damaging publicity and legal costs. They may subsequently be able to recover these costs from their employees or their insurers

Insurance

- The insurers should be informed as soon as a suspicion is raised. In certain circumstances it may be possible to make a claim against the insurers. The person who led the investigation should provide the insurers with any information that is required to substantiate a claim, or to support an attempt by the insurers to secure recovery from the perpetrator.

3.12 Administration

- Careful administration of the investigation is of vital importance. A disordered investigation, without clear records and logs of events, communications, key dates etc, will cause problems at any court hearing, employment tribunal, or disciplinary panel.

- Maintain a chronological record of all events on a main file. This should include all correspondence, telephone calls and emails sent/made and received, interviews, visits, tests/checks undertaken etc.

- Maintain a list of all contacts (eg internal, Police, lawyer, donors/funders, peer organisations, government bodies, and technical advisers).

- Maintain a list of emergency contact numbers and ensure that this is shared with all those on the list.

- Maintain a log of anyone who handles evidence obtained, including the Police.

- Consider whether there is a need for dedicated administrative support; dedicated phone and email address; secure fax machine; secure room etc.

- Do not keep any unnecessary records or copies. Carefully shred any papers that are not needed (e.g. extra copies of progress reports).

- Establish internal and external communication protocols. Discourage the use of email to communicate sensitive information; avoid internal mail and hand deliver highly confidential information, opting for double-enveloped post for less sensitive information. Where email is used for communication, consider entering subject names that have no direct link to the investigation.

- Provide update reports as appropriate to the Head of Internal Audit

3.13 Reporting

- Every investigation of suspected fraud or financial irregularity should result in a report written by the person who led the investigation. This should be done regardless of whether any colleagues are dismissed or prosecutions made and details entered in the fraud register.

- The register will record the scale of the fraud, when and how it was perpetrated and by whom. In addition the report will record; what action has been taken against the perpetrator, the actions to prevent further similar losses and to recover what has been lost. It will also usually be pertinent to note how the fraud was detected and whether or not existing controls were effective.

- Since the report may be used internally for disciplinary hearings or externally for civil or criminal proceedings, conclusions and opinions should be substantiated by evidence.

- It is important to strictly limit the distribution of the report. Copies will not be provided automatically to suspects or their representatives. If a disciplinary hearing takes place the individual and their representative may be entitled to receive a copy subject to obtaining legal advice.

3.14 Review, communication and action on Findings

Review of findings

- The findings reported by the person in charge of the investigation should be reviewed by relevant managers and in particular the lessons learned to avoid future frauds.

- Senior Managers should satisfy themselves that, so far as is practically possible, a similar fraud could not occur again and /or the amount of potential loss has been minimised, the perpetrators have been properly dealt with and recovery has been pursued robustly.

- Managers and supervisors should be disciplined if they have not properly enforced existing controls and procedures.

Communicating outcomes

- Responsibility for communicating findings and actions to those involved and others who need to know should be set out in the Plan. The Council will hold a debriefing once outcomes have been finalised, to ensure that proper closure has been achieved.

- It may be necessary to manage the expectations of the person who raised concerns. The Whistleblowing Policy provides guidance on what may be communicated.

Action on Findings

- Any actions arising from the final report should be allocated to named individuals with appropriate due dates for completion.

- The final details of the fraud should be added to the entry in the Fraud Register.

3.15 Closure

Communication that the case has been closed

- It is important that any decision to close the case is clearly documented and communicated to those involved.

- The case may be closed for a number of reasons, including:

    - All action points that arose from the final report have been completed.
    - The Head of Internal Audit decides there is insufficient evidence to support the allegations.
    - The Council does not wish to incur further costs investigating the case.
    - The decision to close the case and the reason for doing so should be documented by the person leading the investigation and should be added to the investigation file and the fraud register.

Learning from experience

- Following completion of the case, the Head of Internal Audit will prepare a summary report on the outcome and lessons learned, circulating it to all other relevant parties who must take the appropriate action to improve controls to mitigate the scope for future recurrence of the fraud or theft.

Archiving

- All documents associated with the investigation should be archived in a secure location with adequately restricted access, and be retained in line with the document retention guidelines.

- Any redundant documents and papers, or duplicate copies, should be carefully shredded.

Appendix 1 - Examples of fraud

Theft: the illegal taking of someone else's property without that person's freely-given consent. Apart from the obvious theft of Council physical assets such as computers, shop stock and money, it includes:

- Misappropriation of funds
- Misuse of assets, including cash, stock and other assets, for example “borrowing” petty cash, use of photocopiers for private purposes
- Theft from a client or supplier
- Theft of intellectual property (eg unauthorised use of the Council name/logo, theft of product/software designs and client data

Bribery: this implies a sum or gift given or sought that alters the behaviour of the person in ways not consistent with the duties of that person. It includes offering, giving, receiving or soliciting any item of value in order to influence an action.

Corruption: this is a general concept describing any organised, interdependent system in which part of the system is either not performing duties it was originally intended to, or performing them in an improper way, to the detriment of the system's original purpose.

Deception: to intentionally distort the truth in order to mislead others. It would include obtaining property, services or pecuniary advantage by deception or evading liability. Deceptions include:

- misrepresentation of qualifications to obtain employment
- obtaining services dishonestly via technology eg where a credit card that has been improperly obtained is used to obtain services from the internet, or any other situation where false information is provided to a machine
- possessing, making and supplying articles for use in fraud via technology eg computer programs designed to generate credit card details that are then used to commit or facilitate fraud
- undeclared and unauthorised private and consultative work
- failure to properly declare interests that may materially affect the carrying out of their role
- failure to observe, or breaches of, established Council / Service policies, procedures, or practices can in some circumstances constitute an irregularity
- money laundering (see below)
- providing misleading information in order to obtain funds, such as overstating activity

Forgery: this is the making or adapting objects or documents with the desire to deceive.

Extortion: this occurs when a person obtains money or property from another through coercion or intimidation.

Embezzlement: this is the fraudulent appropriation by a person to their own use of property or money entrusted to that person's care but owned by someone else.

False Accounting: this is dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive. It includes:

- Manipulation or misreporting of financial information
- Fraudulent completion of official documents (eg VAT receipts)

Conspiracy: this is an agreement between two or more persons to break the law at some time in the future. It includes breaches of regulations.

Collusion: the term “collusion” covers any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes of fraud.

Money laundering: this is the term used to describe the ways in which criminals process illegal or ‘dirty’ money derived from the proceeds of any illegal activity (eg the proceeds of drug dealing, human trafficking, fraud, theft, tax evasion) through a succession of transactions and deals until the original source of such funds has been obscured and the money take on an appearance of legitimate or ‘clean’ funds.

There are three internationally accepted phases to money laundering:

Placement – this involves the first stage at which funds from the proceeds of crime are introduced into the financial system or used to purchase goods. This is the time at which the funds are most easily detected as being from a criminal source. Such ‘dirty money’ will often be in the form of cash or negotiable instruments such as travellers cheques.
Layering – this is where the funds pass through a number of transactions in order to obscure the origin of the proceeds. These transactions may involve entities such as companies and trusts (often offshore).
Integration – this is when the funds are available via a legitimate source and allow the criminal to enjoy access to the funds again, with little fear of the funds being detected as being from a fraudulent source.

Appendix 2 - Terrorist Financing (Terrorism Act 2000)

Under the Terrorism Act 2000 the assets of charities can be frozen if they are shown to have funded terrorists. Colleagues should therefore be aware of terrorist organisations posing as legitimate entities which can conceal the diversion of funds to terrorist organisations.

Example 1:
An employee working for a charity used his occupation to support the on-going activities of a known terrorist organisation. The employee had secretly made contact with those involved in terrorist activity and used his position to hide weapons and bomb making equipment.

Example 2:
An employee working for a charity obtained surplus funds from the Council to fund terrorism by padding the number of children it had claimed to care for by providing the names of children who were either dead or did not exist. Funds were then diverted to local terrorist organisations. The charity also employed members of the terrorist organisations and facilitated their travel.

Appendix 3 - Examples of controls to prevent and detect fraud

- Thorough recruitment procedures.
- Physical security of assets.
- Clear organisation of responsibilities and reporting lines.
- IT access controls over data
- Adequate staffing levels.
- Supervision and checking of output.
- Separation of duties to ensure that key functions and controls are not performed by the same colleague.
- Rotation of colleagues.
- Random spot checks by managers.
- Regular activity by auditors.
- Complete and secure audit trails.
- Performance monitoring by management.
- Budgetary and other financial reports.
- Reviews by independent bodies such as the the external auditor and Internal Audit.
- Data matching.

Appendix 4 - Warning signs for fraud

There are warning signs that can indicate a fraud may be taking place eg:

- Colleagues under stress without a high workload.
- Reluctance to take annual leave.
- Being first to arrive in the morning and last to leave in the evening.
- Refusal of promotion.
- Unexplained wealth.
- Sudden change of lifestyle.
- Suppliers/contractors who insist on only dealing with one colleague.
- A risk taker or rule breaker.
- Disgruntled at work/not supportive of organisations mission.
- Colleagues with serious financial problems.
- Colleagues whose lifestyle is disproportionate to their income.
- Unusual concerns about visits made by senior managers or auditors.
- Colleagues who often break the rules or fail to comply with procedures.
- Managers/colleagues who cut corners.
- Complaints about colleagues from customers or other colleagues.
- The lack of effective internal controls in an area.
- Unexplained falls in income levels or increases in expenses.
- Deliveries of stocks or orders to other buildings or non-Council buildings.
- Increases in the number of insurance claims.
- A general disregard by management and colleagues towards security.

Fraud Indicators can include:

- Colleagues exhibiting unusual behaviour (see list above).
- False entries in attendance records such as flexi sheets.
- Missing key documents (invoices/contracts).
- Inadequate or no segregation of duties.
- Documentation which is photocopied or missing key information.
- Missing expenditure vouchers.
- Excessive variations to budgets/contracts.
- Bank and ledger reconciliations not regularly performed and balanced.
- Unexplained or unreasonable balancing items in reconciliations
- Numerous adjustments or exceptions.
- Overdue pay or expense advances.
- Duplicate payments.
- Ghost colleagues on payroll.
- Large payments to individuals.
- Crisis management coupled with a pressured work environment.
- Lowest tenders or quotes passed over without adequate explanation.
- Single vendors.
- Climate of fear/low colleague morale.
- Consistent failure to implement key controls.
- Management frequently overriding controls.

Appendix 5 - Fraud / Whistleblowing Register

The Fraud Register contains the following headings:

- Logged By
- Reference Number
- Referred By
- Date Referred
- Details of Referral (Brief)
- Contact Details
- Reported to Monitoring Officer
- Date Acknowledgement letter sent
- Agreed By
- Date Agreed
- Investigating Officer
- Stage / Status of Investigation Outcome
- Date Outcome Reported to Monitoring Officer
- Date Outcome reported to the Whistleblower
- Type of Whistleblowing Date action taken after case finished
- Type of fraud
- Value (£)
- Brief details of the fraud / corruption
- Fraud or Corruption
- Did the case involve an employee or a Councillor?
- Was the person prosecuted?
- Guilty Outcome?
- Outcome
- Perpetrator
- Type of Fraud

Appendix B

Nottingham City Council

Data Matching Strategy and Policy

Nottingham City Council October 2015

Contents

Data Matching Strategy

Data Matching Policy

Page

DATA MATCHING STRATEGY

1. Introduction

1.1 Nottingham City Council is committed to providing the best possible service to its citizens by continually making improvements and utilising resources efficiently and effectively. The Council has access to vast amounts of information and, by making better use of this information across the Council it can enhance services, increase income and work efficiently.

1.2 The ability to match data across the many Council databases can highlight gaps in service provision, identify possible fraudulent activity or streamline processes. The Cabinet Office under its statutory powers has collected data from many public bodies to carry out data matching exercises for the prevention of fraud. This National Fraud Initiative (NFI) has already proved successful by identifying frauds of £1.17 billion since its inception in 1996. Such has been the success of the initiative that many private sector clients now use the service.

1.3 Within the Council, Internal Audit uses data matching techniques in the course of some of its audit investigations. Following the success of data matching exercises it is appropriate that its use be expanded to support the enhanced use of information in the most efficient and effective way to improve the delivery of the service. It is a key objective of Internal Audit to enhance the Council's ability to proactively seek out fraud and error through rigorous, programmed data matching exercises and data mining on areas identified as high risk. Internal Audit will also be seeking a more targeted approach through the better use of intelligence.

1.4 Looking forward, Internal Audit's vision is to expand the use of data matching techniques to include activity on data from other relevant public sector bodies.

2. The key objectives of the Data Matching Strategy

The key objectives of the strategy are:

- Nottingham City Council is committed to the prevention, detection and investigation of all forms of fraud and corruption. Continuous use of data matching in conjunction with auditing will be a pro-active approach to identifying and where possible preventing fraud and corruption. It will:
  - Provide an effective internal control and a means of helping to prevent or identify fraudulent or corrupt activities.
  - Develop an internal tool to help identify errors, inconsistencies, irregularities and risk to financial resources within the Council.
  - Ensure that the Council fully utilises the data held within its systems to best possible effect.
  - Aid the audit planning process and other audit projects.
  - Improve the control environment within the Council.
  - Identify potential weaknesses in design and operation of internal controls that may be creating the risk of fraud or irregularities occurring.
  - Identify potential weaknesses in the design of Information Systems that currently may not provide adequate assurances that they will prevent error or fraud.

- The Council is committed to ensuring its citizens have access to all services they are entitled to. The interrogation of data can highlight areas where there are gaps in service.

- Act in accordance with legislative obligations under the National Fraud Initiative.

- The audit process should be enhanced by:
  - improving the audit planning process and deployment of Audit colleagues
  - using the matching and interrogation of data to highlight areas for further investigation
  - highlighting errors, inconsistencies, irregularities and/or financial risk

- The Council will work within the relevant legislative framework including the Data Protection Act, and Nottingham City Council Information Security policies.

3. Scope of Data Matching

3.1 Data matching and analysis may be performed on any City Council data system.

3.2 Data matching and analysis may be performed on data received from other public bodies by agreement and within relevant legislation.

3.3 In exceptional circumstances data matching and analysis may be performed on data received from other external systems where deemed appropriate to the furtherance of the City Council's anti-fraud objectives and where relevant legislation permits.

3.4 Data matching will be performed routinely as part of our data matching plan, and also on an ad-hoc basis;

Routine Data matching – scheduled data matches may take place on a daily, weekly, monthly or quarterly basis. Datasets will be collected from core systems in accordance with the annual data matching plan.

Ad-hoc data matching – data matches may be required for work of a special nature when routine data matching activities would not be appropriate. Also, data collected for routine data matching activities may also be used as a by-product to drive and support the audit of large information systems.

4. Legal Basis for Data Matching

4.1 In order for the City Council to undertake data matching it must operate within the legislative framework. Internal Audit will work with colleagues in Information Governance and Legal Services to keep abreast of new or amended legislation and ensure the correct procedures are in place to drive improvement.

4.2 Data is currently matched under the following Legislation:

- National Fraud Initiative - Audit Commission Act 1998
- Local Audit and Accountability Act 2014,
- Benefit Counter Fraud – Social Security Act.

4.3 To support internal pro-active anti-Fraud activities, data matching takes place to assist the Section 151 Officer achieve their responsibilities. These are outlined in the Local Government Act 1972 and supported by the internal audit right of access stated in the Accounts and Audit Regulations 2015.

4.4 The City Council will adhere to the Data Protection Act by ensuring there are the relevant fair processing notices in place to inform the data subjects that data matching may take place to help detect and identify fraud.

5. Approach to data matching

5.1 Based upon information obtained from risk analysis work and audit work, an annual data matching strategy will be developed. The strategy will include routine data matching events and leave appropriate contingency to process ad-hoc data matches as their requirement occurs. Risk analysis will be performed from historical information, data trends and other sources of information. Areas with a high fraud risk profile will be targeted.

5.2 The balance of work carried out between routine and non-routine data matching will integrate with existing Nottingham Internal Audit planning objectives.

5.3 Routine data matching will be subject to one time approval. The approval will be reviewed on an annual basis to verify that it remains valid and appropriate. All approvals will require a justification to be produced, outlining the data requirements and data field definitions.

5.4 The overall approach to data matching consists of an extraction of data from any system or data warehouse held by the Council, and then subsequently cross matching or exception testing this data to another data set to help identify potential errors, irregularities or suspect matches.

5.5 Non-routine (ad-hoc) data matches will require approval from the Head of Internal Audit each time a data match is carried out. This will be done prior to approaching the data owner.

6. Retention of data

6.1 The City Council will ensure that data is not held for longer than is necessary for the purpose it was obtained. In establishing retention and archiving periods we will consider both the possibility of complaints and the legal requirements.

6.2 All successful data matches that result in a fraud referral will be documented and retained in line with normal operating procedures.

6.3 Datasets used to carry out data matches will be retained for a maximum of six months after their planned use, subject to the need to conserve evidence.

6.4 All data refreshes will take place on a regular basis ie daily, weekly, monthly or quarterly as relevant to operational needs. Consequently, as the existing dataset will be overwritten, data will only be retained until the following scheduled refresh occurs.

7. Storage of data

7.1 Data is held in secure computer files, which have restricted access.

7.2 Manual records will be held securely in locked filing cabinets.

7.3 Output reports and files that do not highlight a match will be securely destroyed.

7.4 Once the data matching exercise has been completed the extracted source data file will be deleted. Matches which do not identify fraudulent activity will also be deleted. Matches which subsequently highlight fraudulent activity will be maintained for analytical review.

8. Links to Audit Controls and Risk Registers

8.1 Where significant fraudulent activities have occurred through poor system controls, the details will be fed to both the directorate and team responsible, and into the relevant risk register.

8.2 Details will be recorded by Internal Audit to help assess the implications on the annual assurance statement and for future trend analysis.

9. Management Action

9.1 The Head of Internal Audit will make arrangements for follow-up of all positive data matches where a fraud has occurred but no action has yet been taken against the perpetrator(s) of the fraud.

9.2 If no action is taken by a line manager when a fraud or irregularity is proven, the Head of Internal Audit reserves the right to review the fraud circumstances and refer the matter to the City Council's Audit Committee.

DATA MATCHING POLICY

1. Introduction

1.1 Nottingham City Council is committed to quality service provision, reducing the number and value of errors, and reducing the level of financial risk and is continually looking to introduce more efficient and effective techniques to combat fraud. Processes within Internal Audit are designed, where practicable, to add value through techniques including data matching.

1.2 The benefits of data matching are well documented through government initiates such as the National Fraud Initiative (NFI) run s by the Cabinet Office. The NFI forms part of the statutory external audit process for councils, Police and fire authorities in England and Wales. Data matching under the NFI is a legal requirement and audited bodies and other participating organisations supply data for cross-matching between systems to identify cases where fraud may be occurring. Data matching has also been used to identify inconsistencies, for example, where similar information is stored in two different systems and errors resulting from data input.

1.3 Investing in improvement is a key priority for the Council to help it to manage resources economically, efficiently, effectively, flexibly and responsively. Consequently, errors or fraud identified via the data matching route will also help the Council to improve services and the internal control environment, supporting the Council's aspiration to be one of the best run Local Authorities in England.

1.4 Performing data matching and data analysis internally and informing suppliers, partners, colleagues and citizens that it is being carried out may act as a deterrent and create an anti-fraud and corruption culture within the City Council.

2. Definitions

2.1 Data Matching – The computerised comparison of two or more data sets which relate to the same or similar individuals or elements to identify similarities or differences.

2.2 Data Analysis – The process of examining data with the aim of extracting some useful information and identifying anomalies.

2.3 Continuous Auditing – The method that is used to perform control and risk assessments in an automated manner on a more frequent schedule.

3. Purpose of Policy

3.1 To ensure that a consistent data matching approach is adopted across Nottingham Internal Audit by making effective use of a clearly defined strategy and procedures.

3.2 To establish procedures that ensure data matching and analysis is conducted in a controlled, robust and approved manner.

4. Principles of data matching

4.1 The Council will only match and analyse data where relevant legislation permits, in order to avoid unlawful processing of data.

4.2 Data extracted will be obtained in accordance with the Data Protection Act (1998) and, where required, with the consent of the data owner.

4.3 To support the Council's determination to reduce fraud and error it will be Council policy to include a standard declaration in forms or input screens concerning the potential use of data provided to the Council in data matching exercises.

4.4 Only data actually needed to perform the data matching exercise is collected and processed.

4.5 Data matches will be fed into a structured and prioritised programme of activity.

4.6 Source and matched data is only seen by colleagues who need it in the course of their duties.

4.7 The results of a matching exercise do not automatically imply that fraudulent activity has taken place. It highlights areas for further investigation. The investigation team will conduct a thorough review of all results and ensure the accuracy of the data.

4.8 Data found to be inaccurate will be corrected in an appropriate manner so that decisions affecting individuals highlighted in the data matching routine are made on the basis of reliable and up to date data.

4.9 Data matching processes will be refined for future use where indicated by a review of results.

4.10 Data matching outputs are fed, where relevant and appropriate, into the Internal Audit planning process.

4.11 Source data and matched data outputs are protected from unauthorised or accidental disclosure.

4.12 Data is retained only for as long as it is required.

5. Approval

5.1 This policy forms part of the Council's Counter Fraud Strategy which is approved by the Council's Audit Committee.

5.2 The Head of Internal Audit will maintain the policy and review mechanisms set in place to ensure its principles are delivered.

6. Compliance

6.1 Compliance with the policy will be required as part of the Council's Counter Fraud Strategy.

6.2 All relevant colleagues should receive appropriate training to provide an assurance that this policy is understood and followed effectively.

7. Data Retention and Disposal

7.1 Data retention/disposal standards will be in line with Council Information Security Policies.

7.2 Personal information will be safeguarded from accidental and deliberate threats to confidentiality and integrity

8. Policy Review

This policy will be reviewed by the Head of Internal Audit periodically and when relevant legislative changes are enacted.

9. Contact Officer / Guidance

For clarification or guidance in connection with this policy, please use the following contact details

Shail Shah - Head of Internal Audit
Tel: (0115) 8764245
email:shail.shah@nottinghamcity.gov.uk

2 November 2017