



Performance and Audit Scrutiny Committee 24 January 2011

Anti-Money Laundering Policy Revised National Fraud Initiative Strategy Third Quarter Internal Audit Progress Report

SUMMARY

The Committee is asked to:

(a) Anti-Money Laundering Policy

Recommend to Cabinet and full Council that the final Anti-Money Laundering Policy be adopted, and communicated to all staff and Members. **(Annex A)**

(b) Revised National Fraud Initiative Strategy

Note and endorse the content of the revised National Fraud Initiative (NFI) Strategy 2010/11. **(Annex B)**

(c) Third Quarter Internal Audit Progress Report

Note and endorse the contents of the Third Quarter Internal Audit Progress Report for 2010/11. **(Annex C)**

PURPOSE OF THE REPORT

(a) Anti-Money Laundering Policy

To ensure that the council complies with its legal obligations and regulatory responsibilities in respect of anti-money laundering practices.

(b) Revised National Fraud Initiative Strategy

To update members on progress made in relation to actions arising from the NFI Strategy and the updating of the Strategy in line with new guidance from the Audit Commission.

(c) Third Quarter Internal Audit Progress Report

To update members on work undertaken by Internal Audit in the third quarter of the financial year, and the position regarding progress made towards achieving the 2010/11 audit plan presented to this committee on 26 April 2010.

Contact Details

Name

Telephone

E-mail

Chairman

John Hale

01359 221141

john.hale@stedsbc.gov.uk

Internal Audit Manager

Jon Snares

01284 757239

jon.snares@stedsbc.gov.uk

Performance and Audit Scrutiny Committee

24 January 2011

Anti-Money Laundering Policy

1. Purpose of Report

- 1.1 To recommend approval of an Anti-Money Laundering Policy which will ensure the council complies with all relevant legal and regulatory requirements provided for by the UK's anti-terrorist financing and anti money laundering regimes.

2. Background

- 2.1 Money laundering is a term which describes any attempt to use the proceeds of crime for legitimate purposes. Anyone who becomes aware of an activity, which they have reasonable grounds to suspect is related to the proceeds of crime, may be guilty of a money laundering offence, if they do not report their concerns as appropriate.
- 2.2 The legal and regulatory framework for the UK's anti-terrorist financing and anti money laundering arrangements comprises:
- The Terrorism Act 2000;
 - The Proceeds of Crime Act 2002; and
 - The Money Laundering Regulations 2007.
- 2.3 The Chartered Institute of Public Finance and Accountancy (CIPFA) has published guidance on how the provisions of this framework apply to public authorities (CIPFA, 2009). The Anti Money Laundering Policy accompanying this report (Annex A) is designed to ensure that the council and its staff fulfil all legal obligations and regulatory requirements in accordance with this guidance.
- 2.4 Public authorities and their staff are subject to the full provisions of the Terrorism Act and four of the six principal money laundering offences defined in the Proceeds of Crime Act are relevant.

3. Summary

- 3.1 Although the council's risk of exposure to money laundering is relatively low and some of the provisions of the legal and regulatory framework do not apply, there is, as CIPFA observes, a reputational risk for any authority that does not have adequate policies and procedures in place.
- 3.2 CIPFA's view is that, "it is prudent and responsible practice for public service organisations, including those outside the scope of the regulations, to put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements, designed to enable them to detect and avoid involvement in the crimes described in the legislation and regulations."
- 3.3 The risk is not only reputational. There is also a risk that individuals who, in the course of council business, become aware that criminal property or funds could be involved may commit offences under the Terrorism Act or Proceeds of Crime Act sections 327-329 if a reasonable suspicion is not reported.

- 3.4 It is therefore important the council, its staff and Members are protected as far as practicable. Therefore appropriate and proportionate arrangements will be established through the adoption and publicising of this Policy.
- 3.5 Where appropriate, key staff will be provided with training on identifying potential activities and reporting concerns to the Money Laundering Reporting Officer.

Environmental Impact of the Proposal

No environmental impact has been identified.

Equalities Impact of the Proposal

No equalities impact has been identified. Compliance with the proposed policy (Annex A) will ensure that all customers are treated consistently in accordance with the legal requirements related to suspicions of money laundering.

Risk Assessment

Non-compliance with the basic procedures set out in the proposed policy exposes:

- the council to risks of financial loss and reputational damage; and
- individual employees to risks of prosecution (as a party to money laundering offences).

The proposed policy aims to mitigate these risks.

Revised National Fraud Initiative Strategy

4. Purpose of Report

- 4.1 To update members on progress made in relation to actions arising from the NFI Strategy and the updating of the Strategy in line with new guidance from the Audit Commission.
- 4.2 Members are asked to note and endorse the content of the revised National Fraud Initiative (NFI) Strategy 2010/11 (Annex B)

5. Background

- 5.1 Annex B represents an updated version of the National Fraud Initiative (NFI) Strategy for the council. The revised strategy is produced to ensure that the council has the correct procedures in place to meet changes in legislation in relation to data matching and the prevention and detection of fraud. Since the areas included within data matching are expanding and the submission of data has become mandatory since 2008, it is important for the council to have appropriate policies and procedures for officers to follow.
- 5.2 New powers given to the Audit Commission by the Serious Crime Act 2007 enabled the benefits of NFI to be extended to central government and the private sector. The Serious Crime Act 2007 inserts a new Part 2A in to the Audit Commission Act 1998.
- 5.3 The Serious Crime Act imposes a new regulatory regime alongside existing fair processing and other compliance requirements of the Data Protection Act 1998. **In future, any person or body conducting or participating in the Commission's data matching**

exercises must by law, have regard to a statutory Code of Data Matching Practice. The Code of Data Matching 2008 (known as the Code) was laid before parliament during the summer.

- 5.4 The Strategy sets out the key activities and responsibilities for officers in relation to the Code and in relation to the follow-up of matched reports and reporting of progress on the investigation of errors and potential frauds.
- 5.5 An action status report forms part of the Strategy as Appendix 1 and this details actions completed to date and ongoing actions in order to deliver the Strategy and improve the processes that support the NFI objectives.

Environmental Impact of the Strategy

No environmental impact has been identified.

Equalities Impact of the Strategy

An equalities impact assessment was completed when this strategy was first developed. There are positive indicators for the equality impact assessment in terms of the effective use of public funds. The only potential area of concern is the need to ensure that where forms are downloaded, printed or translated into other languages or Braille, then this must include the fair processing notice in order not to inadvertently discriminate against any individuals or groups. An action is included to investigate this matter further.

Risk Assessment

Failure to implement the NFI Strategy; supply correct data in a timely manner to the Audit Commission to allow data sets to be compared; and follow-up and investigate where appropriate matched data reports, could expose the council to financial loss and reputational damage. In addition, it may result in the council failing in its duty to protect the 'public purse' whereby instances of fraud, over-or under-payments and other errors are not being detected.

The proposed strategy aims to mitigate these risks.

Third Quarter Internal Audit Progress Report

6. Purpose of Report

- 6.1 The Chartered Institute of Public Finance and Accountancy (CIPFA) Code of Practice for Internal Audit in Local Government in the UK 2006 (the Code) which has been deemed as proper practice under the Accounts and Audit Regulations 2003, states under 'Standard 10 – Reporting' that 'in addition to the annual report, the Head of Internal Audit should make arrangements for interim reporting to the organisation in the course of the year. Such interim reports should address emerging issues in respect of the whole range of areas to be covered in the annual report'.
- 6.2 The purpose of the report at Annex C is to update members on work undertaken within the third quarter of the financial year and the progress made in achieving the audit plan presented to this committee on 26 April 2010.

7. Background

Role of Internal Audit

- 7.1 Management are responsible for the systems of internal control within the council and should set in place policies and procedures to help ensure that systems function correctly. It is the role of internal audit to review, appraise and report on the effectiveness and efficiency of financial and other management controls, including risk management, corporate governance, and arrangements for providing best value for money. This is achieved by undertaking audits across the full range of the council's functions in accordance with a risk based audit plan which outlines assignments to be carried out and the resources and skills required to deliver the plan.
- 7.2 Internal Audit also undertake other consultancy style work at the request of management, ranging from general financial advice and assistance and financial appraisals of contractors, to involvement in major council initiatives and projects, as well as undertaking special projects and investigations, including investigations into suspected irregularities or fraud.

Requirement for Internal Audit

- 7.3 The Accounts and Audit Regulations 2006 require every local authority to maintain an adequate and effective system of internal audit.
- 7.4 Internal Audit carries out the work to satisfy this legislative requirement, reporting the outcome of its work to this Committee. The Performance and Audit Scrutiny Committee in its role as the council's audit committee has a responsibility for reviewing the council's corporate governance arrangements, including internal control and for scrutinising the Annual Governance Statement prior to its approval at Full Council. The audit work carried out is therefore a key source of assurance that the internal control environment is operating effectively.

Summary of Internal Audit Reports Issued in 2010/11

1. Introduction

- 1.1 Audit reports are issued as final where their contents have been agreed with client management, in particular, responsibility for actions and timescale. During the nine months to date, nineteen audit reviews have been completed to final report stage.
- 1.2 The following sections contain a summary of the content of the internal audit reports issued during the third quarter of the current financial year. Each summary provides an indication of the issues arising from the reviews, as well as action taken in response to previous audit reports.
- 1.3 It should be noted that each summary below represents the situation at the point in time that the audit work was undertaken and therefore it is likely that a number of agreed key improvements will subsequently have been made.
- 1.4 In line with CIPFA good practice guidance, opinions are provided on the operation of control mechanisms where a full audit has been undertaken for the area reviewed. A key to these opinions can be found at the end of this appendix, at Section 8. Where a follow up review has been undertaken full testing of controls will not always be undertaken and therefore an opinion on the operation of controls will not normally be given.

2. Corporate Review of National Indicators

- 2.1 This is an audit review that is undertaken on an annual basis by Internal Audit. The purpose of the audit was to determine whether activities involving the collation, calculation, verification and reporting of National Indicators is in line with recommended practice. A ***substantial assurance*** opinion was provided.

Key areas where improvements are required

- 2.2 Service managers responsible for collating and reporting on performance indicators should ensure that there are adequate written procedures so that in the event of key staff absences this area of work can continue; also roles and responsibilities can be easily shared with new staff and partner organisations. It is acknowledged that procedures have been produced for NI179, following the Internal Audit review of 2009/10.
- 2.3 Service areas with responsibility for National Indicators should consider the adequacy of current arrangements for reporting performance to their related member groups.
- 2.4 Suggestions have been made to improve the robustness of peer challenge for NI188.

3. National Indicators Follow Up

- 3.1 All previously agreed actions for NI 182, satisfaction of businesses with local authority regulation services, have been implemented.
- 3.2 The agreed action for NI 184, food establishments in the area which are broadly compliant with food hygiene law, has been implemented and although collection for this NI is no longer required it has been decided to continue recording this data for internal monitoring.

4. ICT Audit (Internet Controls)

- 4.1 This audit was undertaken to review the adequacy of the council's internet, firewall and website controls. A *substantial assurance* opinion was provided.

Key areas where improvements are required

- 4.2 Whilst an E-mail and Internet Usage Policy is in place, advising of the council's rules for e-mail and access to the internet, the document has not been reviewed since 2006.
- 4.3 An agreement has been entered into with an internet service provider. Points have been raised by both Internal Audit and Legal Services following sight of the agreement, specifically, the section relating to customer data and usage which requires prompt attention. This reinforces the need for Legal Services to have seen and approved the contract prior to it having been signed, as stated in the Contract Procedure Rules.
- 4.4 As part of the Shared Services Project between St Edmundsbury and Forest Heath District Councils staff are beginning to work across both offices, and as such, awareness and compliance against each authority's ICT policies is an area that requires further investigation.

5. West Stow Cash Handling Follow Up

- 5.1 This was a follow up review to an audit report issued in October 2009. Significant progress has been made in tightening controls and addressing the original actions. New actions are agreed to further improve controls in cash handling and procedures.

6. Cash Handling Review – Moyses Hall Follow Up

- 6.1 This was a follow up review to an audit report issued in October 2009. Significant progress has been made in tightening controls and addressing the original actions. New actions are agreed to further improve controls in cash handling and procedures.

7. West Suffolk House Health and Safety Follow Up

- 7.1 This was the first follow up review of progress made towards completing agreed actions arising from the audit report originally issued in December 2009. Almost half of the agreed actions have been implemented; of the remaining actions, two are reliant on working in partnership with a colleague in SCC, which has been hampered by the long term sickness of this key officer, and the remaining actions are currently in progress.

8. Meaning of Opinions given in audit reviews

Meaning of words used: -	
Full Assurance	The full assurance opinion is given where no significant or fundamental recommendations have been made and where controls within the system should provide full assurance that the risks material to the achievement of the system objectives are adequately managed.
Substantial Assurance	The substantial assurance opinion is given where a small number of significant, but no fundamental recommendations have been made and where controls within the system should provide substantial assurance that the risks material to the achievement of the system objectives are adequately managed.
Limited Assurance	The limited assurance opinion is given where a small number of fundamental and also a number of significant recommendations have been made and where controls within the system provide limited assurance that the risks material to the achievement of the system objectives are adequately managed.
No Assurance	The no assurance opinion is given where little or no assurance could be gained from a system where a large number of both fundamental and significant recommendations were proposed and where controls within the system provide little or no assurance that the risks material to the achievement of the system objectives are adequately managed.

ST EDMUNSBURY BOROUGH COUNCIL

ANTI-MONEY LAUNDERING POLICY

1.0 INTRODUCTION

- 1.1 Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for clean money or assets with no obvious link to their criminal origins. It also covers money, however come by, which is used to fund terrorism.
- 1.2 Significant changes to the legislation concerning money laundering (the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003 and 2007) have broadened the definition of money laundering and increased the range of activities caught by the statutory framework.

2.0 SCOPE OF THE POLICY

- 2.1 The Policy aims to maintain and improve upon the high standards of conduct which currently exist within the Council to ensure that third parties are not able to use the council for the purposes of money laundering.
- 2.2 The Policy sets out the procedures which must be followed to enable the Council to comply with its legal obligations.
- 2.3 This Policy applies to all officers (including external appointments, such as consultants) and elected members of the Council. Within this policy the term employees refers to all employees and elected members.
- 2.4 Failure by an employee to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Procedures.
- 2.5 Heads of Service and managers must ensure that all employees are aware of this Policy.
- 2.6 This Policy is to be read in conjunction with the Council's Whistle Blowing Guide and Anti-Fraud and Anti-Corruption Policy.

3.0 PURPOSE

- 3.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This Policy has been written so as to enable the Council to meet the legal requirements in a way which is proportionate to the low risk to the Council of contravening the legislation.

- 3.2 The purpose of this policy is to make all aware of the legislative changes that have been made, their responsibilities regarding these changes, and the consequences of non compliance with this policy.
- 3.3 Potentially any employee could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. This Policy sets out how any concerns should be raised.
- 3.4 Whilst the risk to the Council of contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities: serious criminal sanctions may be imposed for breaches of the legislation.

4.0 THE MONEY LAUNDERING REPORTING OFFICER

- 4.1 The officer within the Council nominated to receive any information regarding possible money laundering activities (the designated Money Laundering Reporting Officer (MLRO)), is the (Internal) Audit Manager. The role of Deputy MLRO is filled by the Principal Auditor.
- 4.2 The MLRO is responsible for deciding whether information received regarding possible money laundering activities should be reported to the Serious Organised Crime Agency (SOCA) and if appropriate make such reports to the SOCA in the form of a Suspicious Activity Report (SAR).
- 4.3 The Internal Audit Section is also available to give advice as required.

5.0 CASH PAYMENTS AND POTENTIAL MONEY LAUNDERING ACTIVITY

Cash Payments

- 5.1 No payment to the Council should automatically be accepted in cash (including notes, coins or travellers' cheques in any currency) if it exceeds £2,000. See paragraphs 6.4 to 6.8 below for further details.
- 5.2 As a general rule staff who collect cash payments are asked to provide the details of any cash transaction over £2000 to the MLRO so that precautionary checks can be performed (see procedure below)

Potential Money Laundering Activity

- 5.3 The following are examples of where extra vigilance should be applied or concerns should be discussed with the MLRO:-
- Any transaction involving an unusually large amount of cash should cause questions to be asked about the source. This will particularly be the case where cash paid exceeds the amount necessary to settle a transaction, and the person(s) concerned request a non-cash return of the excess. This will include double payments.
 - The reason for the use of trusts or offshore funds for handling the proceeds or settlement of a transaction should be questioned.

- Care should be exercised and further enquiries to the MLRO may be needed where:
 - a third party intermediary becomes involved in a transaction
 - the identity of a party is difficult to establish or is undisclosed
 - a vehicle company is used by a third party and the ultimate ownership is concealed or difficult to establish
 - a party is evasive as to the source or destiny of funds.

6.0 DISCLOSURE PROCEDURE

- 6.1 Any employee who knows, suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing must report such matters to the MLRO. The disclosure should preferably be within "hours" of the information coming to the employee's attention or as soon as is practically possible. **Should the employee not do so, then he/she may be liable to prosecution.**
- 6.2 Where an employee knows or suspects money laundering activity is taking/has taken place, or they become concerned that their involvement in a matter may amount to a prohibited act under the legislation, before taking any money they must telephone the MLRO for guidance as soon as possible regardless of the amount being offered.
- 6.3 If an employee has no reason to suspect or know that money laundering activity is taking/has taken place and if the money offered is less than £2000 in cash as payment or part payment for goods/services offered by the Authority then there is no need to seek guidance from the MLRO.
- 6.4 However, if the money offered is £2000 or more in cash then payment must not be accepted until guidance has been received from the MLRO even if this means the person has to be asked to wait. The employee can give the reason for this delay to the person concerned, as they and the council have a responsibility to ensure there is no breach of law.
- 6.5 Before telephoning the MLRO privately for guidance, wherever possible employees should take the name and address of the person offering the cash payment. If the money is subsequently taken a receipt must be issued bearing the name and address of the person paying.
- 6.6 Once an employee has reported their concern to the MLRO they must follow any directions the MLRO may give. **An employee must NOT make any further enquiries into the matter themselves:** any necessary investigation will be undertaken by the SOCA. All members of staff will be required to co-operate with the MLRO and the relevant authorities during any subsequent money laundering investigation.
- 6.7 **An employee's disclosure to the MLRO (or failing that, the deputy MLRO) should be made on the appropriate disclosure form. See Disclosure Form - Part 1, (Appendix 1 of this policy).**

The form must include as much detail as possible, for example

Section 1 – Is this a suspected offence?

Section 2 - Full details of the people involved (including yourself, if relevant), e.g. name, date of birth, address, company names, directorships, phone numbers, etc;

Section 3 -Full details of the type of transaction being dealt with, the nature of their/your involvement. If you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327 – 329 of the 2002 Act, then your report must include all relevant details as you will need consent from SOCA via the MLRO, to take any further part in the transaction. You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g.

- a completion date or court deadline;
- The types of money laundering activity involved: if possible, cite the section number(s) under which the report is being made e.g. a principal money laundering offence under the 2002 Act (or 2000 Act), or general reporting requirement under section 330 of the 2002 Act (or section 21A of the 2000 Act), or both;
- The dates of such activities, including: whether the transactions have happened, are ongoing or are imminent;
- Where they took / are taking place;
- How they were / are being undertaken;
- The (likely) amount of money/assets involved;

Section 4 - Why you are suspicious – the SOCA will require full reasons, together with any other available information to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable him to prepare his report to the SOCA, where appropriate, if reasons for your suspicion are not given to SOCA they may return your form. You should also enclose copies of any relevant supporting documentation

Section 5 – Are you aware of any investigation already being undertaken by your Department or others in relation to this matter.

Section 6 – Examples of who else you may have discussed this with including other staff or team leaders

Section 7 – State full details of who you have contacted, their response / guidance / action to be taken.

Section 8 – If you are a lawyer advising clients in the course of litigation you are exempt from POCA 2002 to report suspicions of money laundering.

Section 9 – Add any other information which you think may be relevant.

- 6.8 Upon receipt of a completed disclosure form (Part 1) the MLRO must note the date of receipt on his section of the form (Part 2) and acknowledge receipt of it. He should also advise the employee of the timescale within which he expects to respond to the employee.

- 6.9 The MLRO will consider the completed form and any other available internal information he thinks relevant e.g.
- reviewing other transaction patterns and volumes;
 - the length of any business relationship involved;
 - the number of any one-off transactions and linked one-off transactions;
 - any identification evidence held; and undertake such other reasonable inquiries (s)he thinks appropriate in order to ensure that all available information is taken into account in deciding whether to report to the SOCA.
- 6.10 Once the MLRO has evaluated the completed disclosure form and any other relevant information, he must make a timely determination as to whether:
- there is actual or suspected money laundering or terrorist financing taking place; or
 - there are reasonable grounds to know or suspect that is the case; and
 - whether he needs to seek consent from the SOCA for a particular transaction to proceed.
- 6.11 Where the MLRO does so conclude, then he must disclose the matter as soon as practicable to the SOCA.
- 6.12 Where the MLRO suspects money laundering but has reasonable cause for non-disclosure, then he must note the report accordingly (the MLRO must liaise with the legal adviser to decide whether there is a reasonable excuse for not reporting the matter to the SOCA), he can then immediately give his consent for any ongoing or imminent transactions to proceed. Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then he shall complete the Form 3 accordingly and give his/her consent for any ongoing or imminent transaction(s) to proceed.
- 6.13 Where consent is required from the SOCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the SOCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the SOCA.
- 6.14 All disclosure reports referred to the MLRO and reports made by him to the SOCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.
- 6.15 **The MLRO commits a criminal offence if he knows or suspects, or has reasonable grounds to do so, through a disclosure being made to him, that another person is engaged in money laundering and he does not disclose this as soon as practicable to the SOCA.**
- 6.16 **At no time and under no circumstances should an employee voice any suspicions** to the person(s) whom they suspect of money laundering, even if the SOCA has given consent to a particular transaction proceeding, otherwise the employee may commit a criminal offence of "tipping off" (see the Guidance Note, Proceeds of Crime (Anti-Money Laundering) – Practical Guidance for Public Service Organisations (CIPFA) for further details). Do not, therefore, make any reference on a client file to a report having been made to the MLRO. Should the client exercise their right to see the file, then such a note will obviously tip them off to the report

having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

7.0 CUSTOMER DUE DILIGENCE PROCEDURE

7.1 Where the Council is carrying out certain 'regulated activities' then extra care needs to be taken to check the identity of the customer or client – this is known as carrying out Customer Due Diligence.

7.2 Customer due diligence means:

- (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
- (c) obtaining information on the purpose and intended nature of the business relationship.

7.3 The Regulations regarding customer due diligence are detailed and complex, but there are some simple questions that will help decide if it is necessary:

- Is the service a regulated activity? (see 7.4)
- Is the Council charging for the service i.e. is it 'by way of business'?
- Is the service being provided to a customer other than a UK public authority?

If the answer to any of these questions is no then there is no need to carry out customer due diligence

If the answer to all these questions is yes then customer due diligence must be carried out before any business is undertaken for that client. If there is uncertainty whether customer due diligence is required then the MLRO should be contacted for advice.

7.4 Regulated activity is defined as the provision 'by way of business' of: advice about tax affairs; accounting services; treasury management, investment or other financial services; audit services; legal services; estate agency; services involving the formation, operation or arrangement of a company or trust or; dealing in goods wherever a transaction involves a cash payment of €15,000 (approx £12,500) or more."

7.5 Where customer due diligence is required then evidence of identity must be sought, for example:

- checking with the customer's website to confirm their business address;
- conducting an on-line search via Companies House to confirm the nature and business of the customer and confirm the identities of any directors;
- seeking evidence from the key contact of their personal identity, for example their passport, and position within the organisation.

- 7.6 The requirement for customer due diligence applies immediately for new customers and should be applied on a risk sensitive basis for existing customers. Ongoing customer due diligence must also be carried out during the life of a business relationship but should be proportionate to the risk of money laundering and terrorist funding, based on the officer's knowledge of the customer and a regular scrutiny of the transactions involved.
- 7.7 If, at any time, it is suspected that a client or customer for whom the Council is currently, or is planning to carry out, a regulated activity is carrying out money laundering or terrorist financing, or has lied about their identity then this must be reported to the MLRO.
- 7.8 In certain circumstances enhanced customer due diligence must be carried out for example where:
- The customer has not been physically present for identification
 - The customer is a politically exposed person
 - There is a beneficial owner who is not the customer – a beneficial owner is any individual who: holds more than 25% of the shares, voting rights or interest in a company, partnership or trust.
- 7.9 Enhanced customer due diligence could include any additional documentation, data or information that will confirm the customer's identity and/or the source of the funds to be used in the business relationship / transaction. If it is believed that enhanced customer due diligence is required then the MLRO should be consulted prior to carrying it out.

8.0 RECORD KEEPING PROCEDURES

- 8.1 Each unit of the Council conducting relevant business must maintain records of
- client identification evidence obtained; and
 - details of all relevant business transactions carried out for clients
- for at least five years. This is so that they may be used as evidence in any subsequent investigation by the authorities into money laundering.
- 8.2 The precise nature of the records is not prescribed by law however they must be capable of providing an audit trail during any subsequent investigation, for example distinguishing the client and the relevant transaction and recording in what form any funds were received or paid. In practice, the business units of the Council will be routinely making records of work carried out for clients in the course of normal business and these should suffice in this regard.
- 8.3 An electronic copy of every customer due diligence record must be sent to the MLRO to meet the requirements of the Regulations and in case of inspection by the relevant supervising body.

9.0 CONCLUSION

- 9.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This Policy has been written so as to enable the Council to

meet the legal requirements in a way which is proportionate to the low risk to the Council of contravening the legislation.

- 9.2 Any concerns whatsoever regarding any transactions should be reported to the MLRO.

10.0 FURTHER INFORMATION

- 10.1 Further information can be obtained from the MLRO and the following sources:

www.soca.gov.uk – website of the Serious and Organised Crime Agency

“Proceeds of Crime (Anti-Money Laundering) – Practical Guidance for Public Service Organisations” – CIPFA

“Anti-Money Laundering (Proceeds of Crime and Terrorism) – Second Interim Guidance for Accountants” – CCAB (**www.ccab.org.uk**)

Money Laundering Guidance at **www.lawsociety.org.uk**

SI 2007 No. 2157 The Money Laundering Regulations 2007 at:

<http://www.hm->

[treasury.gov.uk/consultations_and_legislation/money_laundering_directive/consult_moneylaundering_2007.cfm](http://www.hm-treasury.gov.uk/consultations_and_legislation/money_laundering_directive/consult_moneylaundering_2007.cfm)

(This policy will next be reviewed in 2012, unless it requires early review in the light of shared services)

Disclosure Form - Part 1

Report to Money Laundering Reporting Officer (Internal Audit Manager)

DETAILS OF EMPLOYEE :

From _____
(insert name of employee)

_____ Contact Details _____
(insert post title and Service)

Date _____

1. Are you dealing with a transaction which might be a prohibited act under Part 7 of the Proceeds of Crime Act 2002 and Money Laundering Act 2007 which requires appropriate consent from the SOCA? Yes No

DETAILS OF SUSPECTED OFFENCE :

2. Identities of the person(s) subject to the enquiry

Name _____

Address _____

Contact Details _____
(If a company/public body please include details of nature of business)

3. Nature and details of activity

(Please include full details of activity e.g. what, when, where, how. Continue on a separate sheet if necessary)

4. Nature of suspicions regarding such activity:

(Please continue on a separate sheet if necessary)

5. To your knowledge has any investigation been undertaken?

If yes please include details below:

Yes No

(Please continue on a separate sheet if necessary)

6. Have you discussed your suspicions with anyone else?

If yes please specify below with whom, explaining reasons for

Yes No

such discussion and the outcome of the discussion:

(Please continue on a separate sheet if necessary)

7. Have you consulted any supervisory body for guidance?
(e.g. the Law Society) If yes please provide details:

Yes No

(Please continue on a separate sheet if necessary)

8. Do you feel you have a good reason for not disclosing the
matter to the SOCA? (e.g. are you a lawyer and wish to claim legal
professional privilege?)

Yes No

If yes please set out below full details for not wanting to disclose
the matter
to SOCA ::

(Please continue on a separate sheet if necessary)

9. Please set out below any other information you feel is relevant :

(Please continue on a separate sheet if necessary)

Signed _____ Dated _____

Once completed please forward this form to the Council's MLRO (Internal Audit Manage
Please do not discuss the content of this report with anyone you believe to be involved in t
suspected money laundering activity described. To do so may constitute a tipping off offer
which carries a maximum penalty of 5 years imprisonment.

St Edmundsbury Borough Council

**Draft National Fraud Initiative
(NFI) and Data Matching Strategy**

Version 10

Reviewed and updated 28.10.10

<u>Contents</u>	Page
1. Background	3
2. Scope of this strategy	3
3. Why is NFI and data matching important?	4
4. Our vision and objectives for fraud prevention and detection	5
5. Strategy to deliver NFI and data matching	6
6. Monitoring and review	7
7. Roles and responsibilities	7
8. Supporting guidance and standards	10
9. Supporting Staff	10
10. Security and Confidentiality	10
References	11

Appendix 1: NFI and data matching Action Plan

Further information

For more information on NFI and data matching please contact one of the following officers;

Nicola Parrish
NFI Key Contact
Principal Auditor
01284 757196

Jon Snares
Internal Audit Manager
01284 757239

Liz Watts (NFI Senior Responsible Officer)
Chief Finance Officer
01284 757252

Teresa Halliday
Data Protection Officer
01284 757144

Davina Howes
Policy, Performance and Customer Service Manager
Strategy and Performance (Data Quality Lead Officer)
01284 757070

Information Controller (CMT Rep)
Corporate Director, Community Services
01284 7695

1. Background

- 1.1 A strategy for National Fraud Initiative (NFI) and data matching activities was originally produced in 2008 in response to significant legislative changes surrounding the NFI process. The impact of the changes meant that the number of data sets held within the council that are included in the NFI data matching programme has significantly increased and involvement in NFI is now mandatory. NFI has become much more of a corporate activity. There are a number of set tasks for key officers to complete as well as the investigation of matched data. These tasks also relate to data protection and data security, following recent high profile security breaches. It is therefore important to ensure that roles and responsibilities around NFI and data matching are clearly defined and guidance and information is available to all stakeholders.
- 1.2 On 13 August 2010 the Secretary of State for Communities and Local Government announced the proposed abolition of the Audit Commission. The government has indicated that its aim is for the new arrangements for the audit of local authorities and NHS bodies to be in place from the 2012/13 financial year. The details of the new arrangements and the transition to them have not been worked out and are subject to primary legislation. This is of particular interest since the NFI programme is led by the Audit Commission.
- 1.3 There is no immediate change to the National Fraud Initiative (NFI) and the 2010/11 exercise will continue as planned. The matches from the October 2010 data upload will be available for investigation as planned from 25 January 2011.

NFI Outcomes

- 1.4 £215.6 million of fraud and error identified by the national NFI exercise for 2008/09, represents a 54 per cent increase on the figure of £140 million identified in the 2006/07 NFI exercise, reflecting well on the bodies that followed up effectively the matches given to them. By using data from NHS bodies, local authorities and central government, the national NFI Report 2008/09 exposed:
 - Pension frauds and overpayments amounting to £78 million
 - £56 million of council tax single person discount that was fraudulently or wrongfully received.
 - 181 employees were dismissed or asked to resign because they had no right to work in the UK.
 - 269 people were prosecuted.
 - 21,534 concessionary travel permits and 16,535 blue badges were cancelled.
 - 97 properties were recovered for social housing.
- 1.5 Performance against NFI has been monitored externally through an NFI Audit and the Key Lines of Enquiry (KLOE) by the Audit Commission, although this is likely to be subject to change.

2. Scope of this Strategy

- 2.1 St Edmundsbury Borough Council collects and uses many different types of data from a wide variety of sources, which include customers, stakeholders and partners and other local authorities and government bodies.

- 2.2 It is essential that public bodies have adequate controls in place to prevent and detect fraud and error.
- 2.3 Under its new powers in the Audit Commission Act 1998 Part 2 A, the Audit Commission requires participating bodies (including county and district councils) to submit data for data matching and comply with the Code of Data Matching 2008 (known as the Code).
- 2.4 This Strategy aims to provide a means of ensuring staff have the correct knowledge, understanding and support in order to discharge their NFI roles and responsibilities.
- 2.5 It is important that at the point of data collection, all customers are advised that their information could be passed to the Audit Commission and used for data matching for the detection of errors and fraud. This is known as “fair processing” of data and the requirements of this are set out in the Code.
- 2.6 Compliance with the Code also ensures that correct procedures are adhered to in terms of data matching in relation to the Data Protection Act 1998, and it should be noted that the processing of data by the Commission matching exercise is carried out with statutory authority. It does not require the **consent** of the individuals concerned under the Data Protection Act 1998.
- 2.7 The Strategy has been produced to set out clear objectives for collecting and sharing information for the purposes of data matching and the detection and prevention of fraud and error. The Strategy builds on existing arrangements for the collection of customer data and the matching and review of NFI data.
- 2.8 The Strategy also sets out the key activities and responsibilities for officers in relation to the Code and in relation to follow-up of matched reports and reporting progress on the investigation of errors and potential frauds.
- 2.9 This Strategy should be read in conjunction with the council's Data Quality Policy.

3. Why is NFI and data matching important?

- 3.1 Accurate and reliable information is vital to the success of the organisation. Data is used to:
 - help measure services that we provide to the public;
 - benchmark cost and performance;
 - set targets to improve performance, reduce cost and improve customer care; and
 - data can also be used to identify potential errors and fraud.

The links between NFI data matching reports and data quality are intrinsic and the Audit Commission uses the NFI process to assess the arrangements that audited bodies have put in place to deal with errors and fraud. The Audit Commission also carries out an annual data quality audit to check what arrangements are in place to assure and promote good data quality.

- 3.2 Ensuring good quality data should not be an end in itself but an integral part of our performance management and governance arrangements. By putting both data quality and data matching analysis at the heart of data management systems, greater reliability can be placed on the information we base decisions on and

monitor our performance. The detection of errors can help to identify areas for improvement and will increase the efficiency of the organisation.

3.3 Good data quality and the detection of fraud are important for:

- **Efficiency** - to minimise financial risk (loss of public funds through fraud or overpayments).
- **Performance management** – information is required which will help identify any shortfalls in standards and targets. Accurately reported performance information will help inform sound management decisions.
- **Service improvement** – the detection of errors or fraud will help to identify areas where improvements or additional controls are required.
- **Providing customer confidence** – our stakeholders will have assurance that we have adequate controls in place for the prevention and detection of fraud.
- **Compliance with statutory requirements** – examples include: Data Protection Act 1998, the Code of Data Matching 2008, Local Government Act 1972,

4. Our vision and objectives for fraud prevention and detection

4.1 Vision

Our vision for the detection and prevention of fraud is:-

St Edmundsbury Borough Council is committed to improving internal controls to ensure that data is of high quality and where frauds and errors are detected appropriate action is taken to recover public money and to improve controls.

4.2 Objectives

Our fraud prevention and data matching objectives for NFI are to ensure:-

Governance and leadership

1. that all appropriate staff are aware of their responsibilities concerning data matching and dealing with errors and fraud;
2. that data quality and fraud prevention and detection is embedded within our performance management framework and corporate documents including the corporate plan, service plans, team plans and risk registers;

Procedures

3. systems and procedures are in place so that staff are aware of their responsibilities and the arrangements required to correct errors and deal with fraud;
4. that reporting of NFI issues takes place and any remedial action is reported and monitored;

Systems and processes

5. that all staff use the 'right first time' principle for data capture and that all data is 'fit for purpose';
6. that data is submitted by the only permissible secure method (Data Upload Facility, NFI Website);
7. that all matching is undertaken in a secure manner and that customer and other stakeholders are given appropriate notice of the use of their information;

People and skills

8. the right people with the right skills are involved in data matching processes, investigation of frauds and errors and are reporting outcomes in a timely manner;
9. that all staff involved with NFI have access to relevant training;

Data use and reporting

10. that data is promptly and thoroughly reviewed, and a risk-based approach is taken, particularly where errors may lead to financial loss;
11. that reference is made to NFI guidance on investigating matches before matches are reviewed;
12. that matches are investigated promptly and action is taken to correct any errors;
13. that appropriate action is taken when fraud or corruption is suspected or identified;
14. that all data submission, data review and action for NFI is supported by a clear audit trail and is compliant with relevant legislation;
15. that external inspection and audit standards and requirements are met; and
16. that councillors are informed of the progress of NFI work alongside other internal control reports. (Progress against the NFI Strategy will be reported to the Performance and Audit Scrutiny Committee within the Internal Audit mid year progress report and the Internal Audit Annual Report. These reports feed into the Annual Governance Statement which is also reported to the Performance and Audit Scrutiny Committee and is published with the Annual Statement of Accounts.)

5. Strategy to deliver the NFI and data matching objectives

- 5.1 Our key actions to deliver the NFI and data matching objectives, which have been agreed with the relevant responsible officers, are set out in the NFI and Data Matching Action Plan which is attached as **Appendix 1**. This action plan has been informed by the Audit Commission Key Lines of Enquiry, latest Audit Commission guidance, the Data Protection Act 1998 and the Code of Data Matching 2008.
- 5.2 Risks to achievement of this Strategy should be recorded within the relevant service plans and managed in the normal way. Risks to achievement of NFI

objectives should also be reported to Internal Audit in order for the impact of this to be assessed and reported to the Section 151 Officer.

6. Monitoring and review

- 6.1 Progress against the NFI and Data Matching Action Plan will be subject to bi-annual updates to the Performance and Audit Scrutiny Committee along with progress reports to Management Team, as is the case with other Internal Audit reporting protocols.
- 6.2 The content of the NFI and Data Matching Strategy will be reviewed on a bi-annual basis, to ensure it continues to meet the requirements of Audit Commission or other responsible body and other national guidance.
- 6.3 The NFI Key Contact will monitor performance in relation to the review and investigation of the data matching reports and provide appropriate feedback to managers and the Section 151 Officer (Chief Finance Officer). All Heads of Service must establish appropriate arrangements for managing matched data investigations and NFI recording and reporting in their area.
- 6.4 Internal progress checks will be undertaken as part of the routine audit and review process. It is acknowledged that Internal Audit has an important role in relation to investigating potential fraud and promoting data quality within the council.

7. Roles and responsibilities

- 7.1 The roles and responsibilities for staff and councillors delivering the objectives are set out below;

Councillor Lead	Portfolio Holder for Resources and Efficiency Responsibility for overseeing the management of resources.
Director Lead	Corporate Director Community Services Corporate responsibility for achieving the NFI and data matching objectives.
Section 151 Officer	Chief Finance Officer <ul style="list-style-type: none"> o Senior responsible officer for NFI – key responsibilities to ensure the statutory requirements for bodies participating in NFI are met, as follows: o Nominate a key contact o Ensure the key contact has access via the secure NFI software o Ensure the key contact fulfils all data protection requirements
Heads of Service	Service Leads <ul style="list-style-type: none"> o Responsible for NFI and data matching within their service areas or as appropriate to their disciplines. o Ensuring that sufficient resources are planned and applied in relation to NFI to ensure compliance with Audit Commission and Strategy requirements. o Heads of Service must ensure that staff nominated for NFI responsibilities are allocated adequate time to attend training and to discharge their responsibilities and that arrangements exist to ensure continuity of process in the event of long term absence, role changes or leavers.

	<ul style="list-style-type: none"> o To ensure that adequate resources are allocated to the review and action of matched data reports to ensure all potential errors and frauds are investigated and appropriate action is taken.
Principal Auditor	<p>NFI Key Contact</p> <ul style="list-style-type: none"> o Corporate responsibility to ensure the safe upload of correct data to the NFI website, to lead on NFI activities, to provide support, guidance and training to key employees, as required and to report on non-compliance with the Code of Data Matching requirements. o To nominate data upload and dataset contacts. o To nominate appropriate users that will investigate the matches and act as point of contact for other bodies. o To ensure that data formats guidance and data specifications are adhered to. o To liaise with the Data Protection Officer. o To be the key interface with the Audit Commission on matters relating to NFI. o To monitor progress against NFI matching reports. o To provide feedback on the outcomes of the exercise.
Audit Manager	<ul style="list-style-type: none"> o To ensure that adequate resources are allocated to the management and support of the NFI and data matching processes and Strategy. o To report to councillors (Performance and Audit Scrutiny Committee) bi-annually on progress against the NFI and Data Matching Strategy.
Data Protection Officer	<ul style="list-style-type: none"> o To ensure that appropriate action is taken to inform the Information Commissioner of changes to data responsibilities and access to information. o To provide advice and guidance in relation to Data Protection issues within the NFI processes.
Head of Legal and Democratic Services	<ul style="list-style-type: none"> o To ensure that the council does not breach any legislation or other regulations in its approach to the NFI and Data Matching Strategy. o To approve the release of the Electoral Register.
Head of HR and Organisational Development	<ul style="list-style-type: none"> o To progress any action in relation to staff implication in fraud and corruption matters. o To support training activities developed to improve NFI actions.
Other Staff	<p>Data Leads (referred to by Audit Commission as download and data set contacts)</p> <ul style="list-style-type: none"> o Responsible for ensuring that fair processing notices are applied in a timely manner for data sets, and personally responsible for data submission: <ul style="list-style-type: none"> ▪ In accordance with the specifications; ▪ In the correct format; and ▪ By the specified submission method (Data File Upload) (including involvement in verifying the format of data for submission and leading the investigation matched report reviews for their data set). o Personally responsible for investigation of matches and updating the NFI database, as appropriate and for liaising with other bodies in relation to matches.

ICT (ICT and e-Services Manager, Systems Development and ICT Security Manager)	<ul style="list-style-type: none"> o Responsible for the technical support in order to extract data (in the appropriate format and within specified timeframes). o Support the upload to the NFI web-enabled database, where this is required.
---	--

7.2 It is the responsibility of each Data Lead to inform the NFI Key Contact of any changes to the key systems or staff in the following table so that any potential NFI issues can be identified and dealt with at an early stage.

7.3 The Data Leads for 2010/12 are detailed as follows:-

Data Required	Data Leads	System/Software
Payroll	Teresa Stace/Jackie Young	iTrent (NT WINDOWS)
Pensions payroll (Data supplied by SCC/CSD)		Axis
Trade creditors' payment history and standing data	Melissa Evans/Linda Manning	E5
Housing (Data currently supplied by Havebury)	Carole Herries	LOCATA Abitas
Housing benefits	Ann Parry-Jones/Sue Archer	Northgate
Council tax	Ann Parry-Jones/Debbie Peckham	Northgate
Electoral register	Fiona Osman (Joy Bowes for approving extraction)	Express
Transport passes and permits <i>residents' parking</i>	Steve Boor/Jacky Martin/	Excel spreadsheet
Transport passes and permits <i>concessionary fares</i>	Ivan Sams/Teresa Claydon/Pam Veal * Changes expected from 01.04.2011	FareDeal
Insurance claimants	C Barber/Michelle Rolls/Sharon Rose * Data also provided by Zurich wef 1.04.2010	LACHS (Local Authoritys Claims Handling System)
Licences <i>Taxi driver and (new) Personal licences to supply alcohol</i>	Carole Herries/Hilary Workman	Flovate/M3 LALPAC (wef 01.04.10)
Licences <i>Market trader/operator</i>	Head of Planning/Cameron Findlay	Excel spreadsheet

8. Supporting guidance and standards

8.1 The [Audit Commission website](#) and the NFI Database provide a vast amount of guidance and information on NFI, data matching and the investigation processes **and in all instances** these websites should be the first point of reference for any guidance or information. A queries email address nfiqueries@audit-commission

.gov.uk is also available. Periodic newsletters are produced by NFI (*NFI Matters*) and these will be circulated by the NFI Key Contact. If there are difficulties in obtaining access to these websites, support should be requested from the Internal Audit Team.

- 8.2 Fair Processing Notices must be issued under the Code. The standard wording advised by the Audit Commission should be used wherever possible and deviations from this should be checked with both Legal Services and Internal Audit. Guidance on Fair Processing Notices is provided by the Audit Commission via the secure website facility and also within the [Code of Data Matching](#). The Summary Notice should be provided to all individuals whose data is to be matched. Where practicable it should point to where more detailed information can be found, for example, by providing web-links to the Condensed Text on the councils website and subsequent links to the Full Text on the Audit Commission website, or contact details for a named person such as the key contact or Data Protection Officer. ***Where an application form is used to collect the data, the summary notice should usually be included on this form.***

Employees should be notified both at the time of the original application for their post and before each NFI exercise, for example, by including a summary notice in their payslip.

9. Supporting staff

- 9.1 The provision of training and development for staff is key to the achievement of the NFI and Data Matching Strategy. To support this, Internal Audit staff can provide guidance, support and training on the use of the NFI interactive database. Online training modules are also available within the database itself and therefore Data Leads should ensure that these have been completed in advance of any investigatory actions in order to maximise the benefits of the approach. It is the responsibility of Heads of Service to ensure that staff involved in NFI have read and understood the NFI instructions and the further database guidance on the meaning of matched reports and the correct approaches to investigation. Staff involved in NFI should be allocated appropriate time in order to investigate matched reports. Further guidance can be sought from the Key Contact or other members of Internal Audit.

10. Security and Confidentiality

- 10.1 We are committed to keeping data secure and confidential where appropriate. Our ICT Security Policy was reviewed in February 2010 and contains guidelines to help staff avoid storing unnecessary and unwanted data in the wrong place. The NFI Strategy considers data security in line with the Code of Data Matching Practice 2008 and therefore the following principles should be adopted in relation to NFI data matching processes:-
- Data obtained for the purpose of data matching exercises may not be disclosed unless there is legal authority for so doing. This applies equally to data obtained for the purposes of matching and the results of the data matching.
 - Results of data matching may only be disclosed further if it is to assist in the prevention and detection of fraud, to investigate or prosecute an offence, for

the purpose of disclosure to an auditor (Audit Commission) or otherwise as required by statute.

- Any disclosure in breach of the principles under section 2.15 of the Code is a criminal offence.

- 10.2 All staff involved in NFI and data matching should have regard for the Code, and in particular sections **2.10 Security, 2.11 Supply of data, 2.15 Disclosure of data and 2.18 Retention of Data**.
- 10.3 Investigating officers and data leads should ensure that copies of matched reports are not held on systems for any longer than investigation requires and that these reports are not held on memory sticks, C Drives or personal drives. This is also a requirement under the ICT Security Policy.
- 10.4 Staff with access to the NFI reporting site should ensure that all passwords are held securely and are **not** shared with other employees. Where additional access to the database is required, permission should be directly requested via the NFI Key Contact or the Internal Audit Manager.
- 10.5 Where any data matching reports are printed, these should be held securely in locked storage in a secure environment and should be only accessible to named individuals (2.13.3).
- 10.6 **All staff** involved with NFI should ensure that data is only uploaded via the DFU Facility on the NFI Website. ***This is now the only acceptable method of data submission for NFI data. If any other method of submission is used, it is the Audit Commission's policy to inform the Director of Finance¹ that data has been put at unnecessary risk.***

References

Code of Data Matching Practice July 2008
(Audit Commission, October 2010)

National Fraud Initiative 2008/09
Public Sector National Report
(Audit Commission, October 2010)

National Fraud Initiative 2010/11 Instructions - England
(Audit Commission, September 2010)

Policy Review

This policy will next be reviewed in 2012, unless it requires early review in the light of shared services.

¹ The role of Director of Finance at the council, for the purpose of NFI, is taken to be the Chief Finance Officer.

NFI and Data Matching Action Status Report

This plan sets out actions to be taken to deliver the NFI and Data Matching objectives as set out in the NFI and Data Matching Strategy. The Actions will be monitored by the Audit Manager and progress reported to the Performance and Audit Scrutiny Committee on a biannual basis.

No	Action	Lead Officers	Timescale	Comments/Further Actions
Governance and Leadership				
1.	Roles and Responsibilities for NFI for 2010-2012 to be clarified within revised Strategy following new guidance from Audit Commission	NFI Key Contact/CFO	January 2011	<ul style="list-style-type: none"> Confirmed in responses to revision of Strategy COMPLETE NFI Website Updated with details of Data Leads (Upload Contacts and Data Set Representatives) COMPLETE Revised Strategy approved and promoted.
2.	Accountability for NFI to be recorded through performance process.	Heads of Service	March 2011	<ul style="list-style-type: none"> This would ideally need to be in place in advance of dealing with data matching reports. To be picked up via service plans and individual target setting – led by HOS
3.	Data Protection Officer to inform Information Commissioner of use of information by Audit Commission and Auditors as recipients (see pg 13, 2.4.7)	Data Protection Officer	ASAP COMPLETE	<ul style="list-style-type: none"> Failure to do so will put St Eds in breach of the Data Protection Act 1998 Data Protection Officer aware that this action needs to be completed 1.11.10. These changes are implemented via the Information Commissioners website and review of this has been completed and confirmation that the title ‘Auditor’ covers this purpose has been received from the Information Commissioners Office.
Policies				
4.	NFI Data Leads and other responsible officers to comment on content of the revised NFI Strategy and Action Plan	All managers with NFI responsibilities	December 2010	<ul style="list-style-type: none"> Member lead to be informed of contents of completed draft Strategy. Strategy & Action Plan to be agreed by Data Leads and Service Leads in advance of MT Comments to be considered and audit trail of officer involvement for External Audit review.
5.	Ensure a system is in place for formal top level and committee reporting on NFI and data quality issues and improvement actions.	Internal Audit	ONGOING	<ul style="list-style-type: none"> Top level reporting to MT to be actioned via Internal Audit report which goes to Performance and Audit Scrutiny Committee three times a year. Annual data quality review paper to be presented to Performance and Audit Scrutiny Committee which will cover non compliance/weaknesses and action taken.

No	Action	Lead Officers	Timescale	Comments/Further Actions
Systems and processes				
6.	<u>Fair Processing Notices</u>	All Data Leads/Website Manager/ICT	ONGOING	<ul style="list-style-type: none"> ▪ We must comply with this in order to meet both Data Protection and NFI requirements (Key Contact required to report to NFI on compliance in September) COMPLETED FOR 2010/11 ▪ Compliance with fair processing to be confirmed via email and links to evidence provided – in order to report back to NFI COMPLETED FOR 2010/11 ▪ Website contains condensed Text and links to further information and full text on the NFI Website and also contact details within the Audit Commission. COMPLETED
a.	To be actioned for all electronic and manual forms collating data for statutory data sets (see data requirements sheet from NFI) Note: 2.8.17 – retrospective for some data			
b.	Website to contain Level 2 Notice and links to Level 3 Notice			
c.	Form 3 Fair Processing Compliance Return completed and returned to NFI.			
7.	<u>Data Extraction</u>	Heads of Service/NFI Data Leads	October 2010 ONGOING	<ul style="list-style-type: none"> ▪ Actions to be completed asap in case additional support is required from software suppliers ▪ Learning from start of 2010 exercise to be summarised and discussed with key NFI stakeholders and participants
a.	NFI data leads and ICT lead to read and understand data extraction requirements for their system and to set up action call with ICT/make any further arrangements necessary with software supplier.			
b.	NFI data leads to understand issues previously identified with data extraction for their system.			
c.	This information available via NFI Database. (2.9.1 and 2.9.2) Data Leads to confirm with Key Contact completion of these two tasks, via email.			

No	Action	Lead Officers	Timescale	Comments/Further Actions
8.	Data Extraction ICT to ensure that there is adequate expertise and support available to provide NFI with data uploads within statutory deadlines.	ICT and eServices Manager	ONGOING with new extractions	<ul style="list-style-type: none"> Need to ensure resource is available since this is statutory requirement – needs to be balanced with Shared Services work for future extractions.
9.	Data Extraction ICT/Data Leads to check data extraction reports prior to verification by Key contact (2.9.2 and 2.9.3)	Data Leads/NFI Key Contact	September 2012	<ul style="list-style-type: none"> Not actioned by Data Leads in October 2010. Data quality checks implemented by Internal Audit, prior to data upload, identified that a number of issues existed with the quality and presentation format of the data. See comments under Action 7. Further training and guidance to be provided prior to the next upload. To Note: the date could be subject to change.
10.	Service Planning The risk of not allocating enough resource to NFI for investigating matched reports needs to be considered within service planning process.	Heads of Service/Risk Manager/ Policy, Performance and Customer Services Manager	December 2010 ONGOING	<ul style="list-style-type: none"> Need to ensure resource is available since this is statutory requirement and adds value where errors and false claims are identified and incidences of fraud are dealt with. Issues highlighted via email to senior responsible officer for NFI where NFI report on inactivity within the database.
People and Skills				
11.	Roles and responsibilities for data quality are clearly defined within the performance management system (PDRs) so that training needs are identified and resource allocation is built into service planning. (Also see Action 1)	HOS/All Managers	April 2010 ONGOING	<ul style="list-style-type: none"> Use the Performance Development Review process to identify individuals' roles and responsibilities and to monitor compliance. Note: data quality was explored during the review of the Performance Development Review process in 08/09
12.	Ensure adequate support and training is available for all staff involved with NFI matched reports and data submission.	NFI Key Contact/Internal Audit Manager	August 2010 ONGOING	<ul style="list-style-type: none"> General guidance on NFI to be provided through Data Leads, ensuring that the relevant staff are made aware of the NFI and Data Matching Strategy. Training will be identified and allocated as required. NFI Database training modules to be completed by Data Leads.

No	Action	Lead Officers	Timescale	Comments/Further Actions
Monitoring and Review				
13.	<u>Progress on fair processing</u> Forms and Website Review to ensure compliance and sign off to Audit Commission.	NFI Key Contact/CFO	September 2010 COMPLETE	<ul style="list-style-type: none"> KEY CONTACT will need separate confirmation of actions taken for each data set area in order to provide a full audit trail of evidence of sign off. COMPLETE Completed and electronic sign off – 21/09/2010 COMPLETE
14.	<u>Data Submission</u> All statutory data requested has been successfully checked and uploaded to NFI database.	NFI Key Contact/Audit Manager	October 2010 COMPLETE	<ul style="list-style-type: none"> Statistics held by Audit Commission to support CAA (UoR) judgements. Upload for 2010 completed within required deadlines.
15.	<u>Equality Impact Assessment</u>	Website and Publications Officer	March 2011	<ul style="list-style-type: none"> To ensure that where forms are downloaded, printed or translated into other languages or Braille, then this must include the fair processing notice in order not to inadvertently discriminate against any individuals or groups.
16.	<u>Policy Review</u> Policy to be reviewed in 2 years in light of potential changes with Audit Commission and shared services agenda.	CFO/NFI Key Contact	OCTOBER 2012	<ul style="list-style-type: none"> NFI Key Contact to monitor changes with Audit Commission and identify opportunities of shared processes with FHDC.

Third Quarter Internal Audit Progress Report

1. Review of Internal Audit work for the nine months to December 2010

1.1 An overview of the work of Internal Audit for the third quarter of 2010/11, and progress made towards achieving the audit plan for the year, is set out below.

2. Corporate work including work on behalf of the Chief Finance Officer

2.1 During the third quarter of the financial year 2010/11 Internal Audit involvement in corporate work has included the following:

- Ongoing membership and contribution to the Strategic Risk Management Group and Performance Management Group;
- Attendance at Management Team meetings to brief senior managers in relation to the outcomes of work undertaken by the section where corporate issues are covered;
- Supporting the Shared Services Programme with the Principal Auditor taking on the role of a Shared Services Architect (SSA) and the Senior Auditor supporting the work of the Finance Workstream. The SSA role has included the planning and delivery of a number of workshops to identify stakeholder needs, risk, and to develop a vision for the service under review. The Senior Auditor has been supporting a working group looking at the development of an information sharing protocol.
- Responding to four requests for financial vetting or other related financial advice including assessments of organisations' financial suitability to undertake specified contracts. We have now responded to twenty such requests in the year to date;
- Continuing to provide advice to service areas on internal controls.

3. Core Financial Systems and Fundamental Review Work

3.1 This work is concerned with the documentation, evaluation and testing of the effectiveness of systems of internal control within the council's financial and information systems, including compliance with the council's rules and policies and its overall risk management and corporate governance arrangements.

3.2 We have agreed with the Audit Commission to commence the majority of this work during the latter six months of the financial year to enable them to place as much reliance on the work of Internal Audit as possible, resulting in potentially reduced Audit Commission testing and slightly lower fees, while still giving Internal Audit a realistic chance of completing the statutory Audit Plan (that is, the core financial systems reviews).

3.3 Six of these audit reviews have been completed and issued as final reports, these being:

- Data Protection Arrangements
- ICT Audit (Disaster Recovery Follow Up)
- ICT Audit (Laptop Security Follow Up)
- Corporate Review of National Indicators

- National Indicators (Follow Up)
- ICT Audit (Internet Controls)

The results of the first three of these audits were reported to this Committee in summary form at the October 2010 meeting while the latter three are shown in summary form at Appendix A.

- 3.4 Three of the fundamental systems audits are at the stage where testing has been completed and we are awaiting agreement of draft reports and agreed action plans:
- Council Tax
 - Non Domestic Rates
 - Contract Procedures

- 3.5 A number of audit reviews have audit testing in progress, they include:
- Housing and Council Tax Benefits
 - Accounts Payable
 - National Indicators
 - Payroll
 - Human Resources
 - Main Accounting System

The results of the audits referred to in paragraphs 3.4 and 3.5 above, as well as audits not yet commenced, will be reported to Performance and Audit Scrutiny members in the Annual Internal Audit Report in April 2011.

4. Departmental Systems Reviews and Probity Audits

- 4.1 This work is concerned with reviewing internal controls within departmental systems, areas for review being identified by a risk analysis undertaken before the start of the financial year.
- 4.2 During the first nine months of the financial year 2010/11 thirteen internal audit reports have been issued within this category, namely:
- Grants Paid
 - Fees and Charges
 - Bury Bus Station Cash Handling Follow Up
 - Tourist Information Cash Handling Follow Up
 - Concessionary Bus Travel Follow Up
 - West Suffolk House Building Security Follow Up
 - West Suffolk House Car Parking Follow Up
 - Parks Follow Up
 - Partnerships Follow Up
 - Car Parks Follow Up
 - West Stow Cash Handling Follow Up
 - Moyses Hall Cash Handling Follow Up
 - West Suffolk House Health and Safety Follow Up

The first ten of these audits were reported to this Committee in summary form at the October 2010 meeting while the latter three are shown in summary form at Appendix A.

- 4.3 Work is continuing on raising fraud awareness within the council, for example, a message has been put in the council's internal bulletin reminding staff of their responsibilities regarding gifts and hospitality.

5. Performance

Utilisation of Audit Time

- 5.1 Internal Audit continues to have a full staff complement and we are on track to achieve the statutory Audit Plan.

Partnership Working – Suffolk Working Audit Partnership

- 5.2 Internal Audit actively contributes to the Suffolk Working Audit Partnership (SWAP). This partnership allows local authorities in Suffolk to share resources, knowledge, and experience regarding internal audit issues in order to identify and promote the adoption of best practice, primarily through an extranet facility. The partnership identifies common training needs and initiates joint training where necessary. This is all achieved at minimal cost.

6. Partnership Working – Shared Services

- 6.1 In order to ensure that Internal Audit make further progress towards working more closely with Forest Heath District Council a number of initiatives have already taken place, including agreeing that Internal Audit liaison meetings with the Audit Commission will now be held jointly by the two authorities, and the annual audit planning process will start earlier in the year to allow both Audit Managers to jointly consider opportunities for reciprocal and joint audit work at each authority. In addition, CIPFA's draft Statement on the Role of the Head of Internal Audit is being jointly considered by both Audit Managers to ensure that efforts to achieve continuous improvement of each internal audit service are made in the context of the shared services agenda. A Collaborative Outcomes workshop was also attended by both teams to start exploring ways in which we could begin to work closer together. A number of ongoing actions were agreed following this activity.
- 6.2 In addition, the Suffolk Chief Executives have identified Internal Audit as one of the services that could be delivered more efficiently across all councils through a shared approach. In order to take this forward a Suffolk Internal Audit Partnership Board has been established to lead the process. The Board members meet on a regular basis, and provide progress reports to the Suffolk Chief Finance Officers.