APPENDIX A

Leicestershire County Council

Internal Audit & Assurance Service

Annual Counter Fraud Report (April 2024 – March 2025)

Leicestershire County Council Internal Audit & Assurance Service

Annual Counter Fraud Report (April 2024 – March 2025)

1. Introduction

This report seeks to summarise the counter fraud activity that has taken place within the County Council during the 2024/25 financial year.

Fraud is a significant risk to the public purse and the Council has a responsibility to prevent, detect and deter fraud related activity. It does this through its counter-fraud service, undertaking both proactive (planned) and reactive (demand led) activity. This is coordinated through the Internal Audit & Assurance Service, Corporate Resources Department. Reactive work is not solely restricted to fraud investigations but extends to other investigatory work, e.g. management commissioned reviews into process failings.

Within its Terms of Reference, the Corporate Governance Committee has a responsibility to monitor the effectiveness of the Council's arrangements for combating fraud and corruption and the approval of relevant policies.

2. Fraud Landscape

Fraud and error cost the taxpayer billions of pounds each year – but most of the potential loss goes undetected. Based on the Public Sector Fraud Authority's (PSFA) methodology, the National Audit Office (NAO) estimates that fraud and error cost the taxpayer £55 billion to £81 billion in 2023-24. Only a fraction of this is detected and known about – enabling investigation and recovery.

Local authorities continue to face significant fraud challenges and whilst the official figures specific to just LAs are at times dated the importance of protecting funds and vulnerable people remains. Tackling fraud is an integral part of ensuring that tax-payers money is used to protect resources for frontline services. The Local Government Transparency Code includes an estimation that the cost of fraud to local government is in the region of £2.1

billion a year. This is money that can be better used to support the delivery of front-line services and make savings for local taxpayers.

The Government's Economic Crime Plan states that the numbers of fraud offences rose by 12% during 2018 to 3.6 million – constituting a third of all crimes in the UK. Although an outdated figure, and whilst we do not have a wholly reliable estimate of the total scale of economic crime, assessments within the public and private sectors indicate that the scale of the economic crime threat continues to grow.

As an upper-tier local authority, the Council does not have exposure to some of the high-volume, high-risk, fraud areas that typically affect district and unitary councils, such as Council Tax, Housing Tenancy or Right to Buy, which comprise a significant proportion of the total national picture.

Fraud is a significant risk for all organisations and local government is no different. Fraud can be internally perpetrated (insider fraud or employee fraud) or externally perpetrated. Indeed, it could be a blend of internal and external factors, e.g. through collusion.

3. Zero-Tolerance Approach to Fraud & Corruption

The Council has a published **zero-tolerance** approach to all forms of fraud, corruption and other financial irregularities. The Council will take all necessary steps to identify, investigate and disrupt instances of fraud and take appropriate action against any individuals or organisations involved in fraud or corruption. This may include internal disciplinary action, dismissal, referral to law enforcement agencies, deregistration applications (e.g. with professional bodies), cessation of provision of services to a client (service user) involved in fraudulent activity, contract termination regarding a provider or supplier involved in fraudulent activity, loss recovery action, etc.

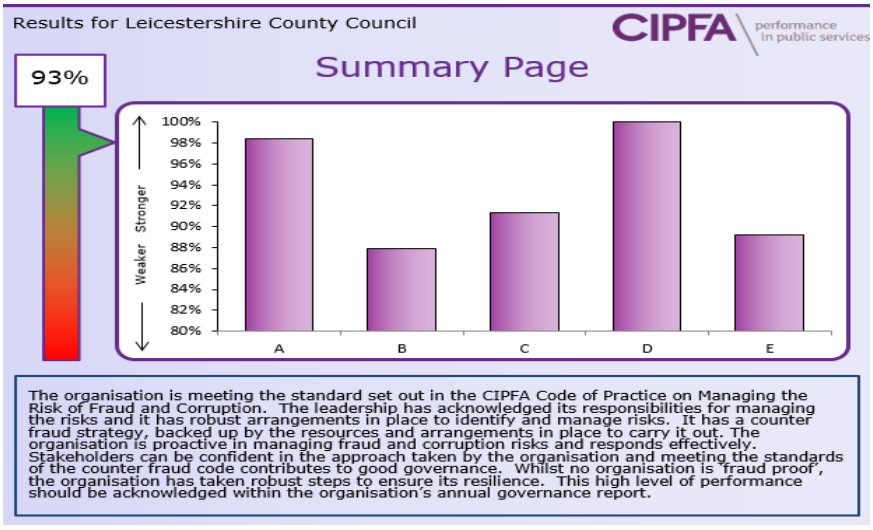
The Council fully recognises its responsibility for spending public money and holding public assets. The prevention, and if necessary, the investigation, of fraud and corruption is therefore seen as an important aspect of its duties which it is committed to undertake.

4. Assessment against the CIPFA Code of Practice – Managing the Risk of Fraud & Corruption

The Council seeks to regularly self-assess its counter fraud approach against the CIPFA Code of Practice – 'Managing the Risk of Fraud and Corruption' (the Code). Assessment is not mandatory but is recommended as good practice. Leaders of public sector organisations have a responsibility to embed effective standards for countering fraud and corruption. This supports good governance and demonstrates effective financial stewardship and strong public financial management. The five key principles of the Code are to:

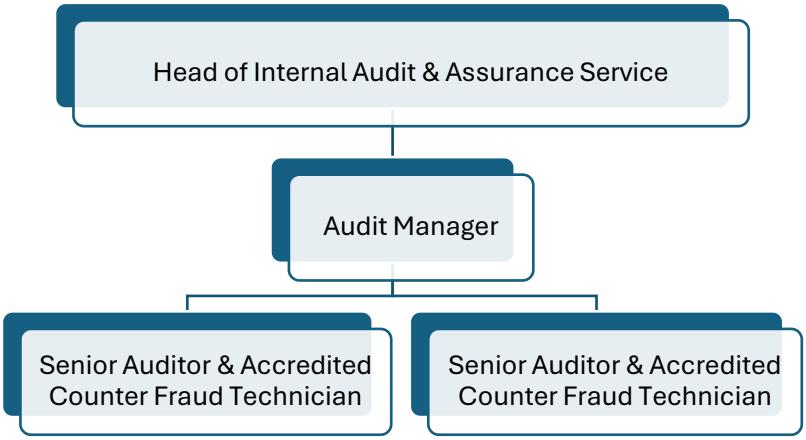
A - Acknowledge the responsibility of the governing body for countering fraud and corruption
B - Identify the fraud and corruption risks
C - Develop an appropriate counter fraud and corruption strategy
D - Provide resources to implement the strategy
E - Take action in response to fraud and corruption.

The most recent assessment was undertaken in 2023. The assessment method is primarily through self-evaluation; however, the Council decided to arrange for the assessment to be peer reviewed by the Corporate Investigation Manager from a neighbouring council to independently stress-test the results/conclusions and to check that these were reasonable. The results of the 2023 assessment were overall positive with the recommendations arising from the assessment now implemented.



5. Counter Fraud Resources

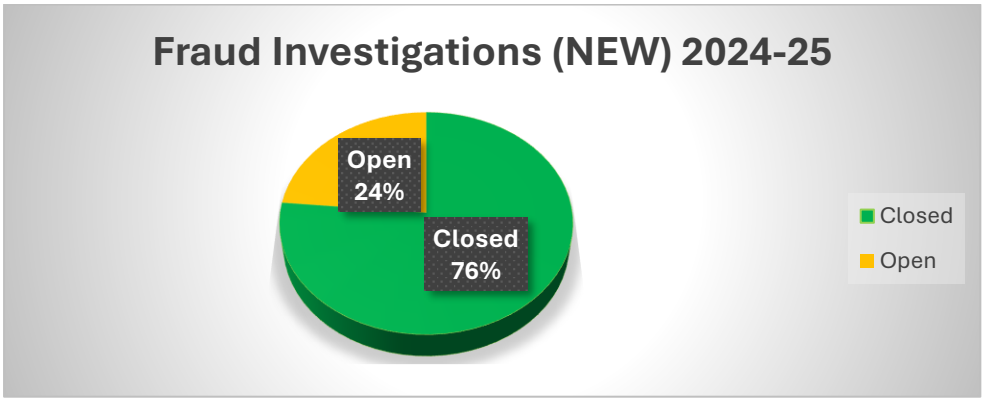
Strategic responsibility for counter fraud rests with the Head of Internal Audit and Assurance Service. Within the team, two senior auditors hold the CIPFA Counter Fraud Technician qualification. These two members of staff report to an Audit Manager who gives managerial oversight. Other auditors and relevant specialists are called upon to provide assistance as required.



Counter fraud work is both proactive (planned) and reactive (i.e. demand-led, e.g. investigations). For the 2024/25 financial year, the total time incurred on counter fraud work was 126 days (45 proactive and 81 reactive). The two senior auditors devoted almost 100 days (approximately 30% of their resource net of overheads and work for other clients).

6. Number and Status of New Investigations Commencing in 2024/25

New Fraud Investigations Commencing in 2024/25 (*)	17	100%
Number Closed at Year-End	13	76%
Number Remaining Open at Year-End	4	24%



Whilst it is desirable for fraud investigations to be closed down promptly, this is not always possible, e.g. in complex investigations or investigations involving law enforcement agencies. It is, therefore, not unusual for some fraud investigations to straddle more than one financial year.

(*) n.b. the metrics shown above also include any cases determined upon investigation to not be fraudulent in nature but which started off as fraud investigations at the outset. The metrics do not include non-fraud work, e.g. management commissioned reviews into process failings.

7. Undertaking Fraud Investigations

Responsibility for undertaking fraud investigations will depend upon several factors, e.g. the complexity of the matter under investigation. Some will be departmentally led by managers, with oversight and support from the Internal Audit & Assurance Service and other relevant stakeholders such as Human Resources and Legal Services. In some cases, the Internal Audit & Assurance Service may lead on the investigation, whilst in others it may be other specialist officers, e.g. ICT Services, or on some occasions an externally commissioned resource. A strategy meeting of relevant officers may determine that a discussion is required with Leicestershire Police.

8. Summary of Investigations Closed in 2024/25 by type/category

2024/25 Investigations Closed During 2024/25	13
Prior Year Investigations Closed During 2024/25	8
TOTAL NUMBER CLOSED DURING 2024/25	21

A summary of themes in relation to common fraud risks and investigations undertaken includes the following (n.b. it would be inappropriate at this stage to discuss details of *ongoing* investigations):

Procurement. Exposure to procurement fraud could be in several areas, including the tendering and contract award stage and the post-contract award stage, e.g. overcharging, duplicate payments, etc. No fraud was identified during the year; however, procurement remains a significant focus and the Internal Audit & Assurance Service has been involved in brokering

process changes in several areas to further fraud-proof systems and processes.

Employee / Insider Fraud. Insider fraud can take many forms, e.g. travel claims, theft, absence fraud, recruitment fraud, etc. A small number of low-level issues arose during the year, and appropriate action was taken in all cases in line with HR and other policies.

Cyber Fraud. Cyber fraud can take many forms, e.g. mandate fraud, "bogus boss" fraud, payment redirection fraud, phishing attempts, etc. A small number of low-level issues arose during the year, and were dealt with as appropriate, with no financial loss to the Council. These were low impact issues causing inconvenience rather than breach of data.

Social Care. Social care fraud can include direct payments fraud, deprivation / non-declaration of assets and financial abuse of vulnerable service users (safeguarding). No fraud was identified during the year. Proactive audit work took place in major risk areas during the year leading to the brokering of process changes in several areas to further fraud-proof systems and processes.

Grants Payable. Grant fraud can comprise bogus or exaggerated applications or misspend of grant. One instance was referred to Action Fraud. Internal processes were strengthened as a result. A further case was unsubstantiated upon investigation.

Council funding of external providers. This can comprise false or exaggerated claims or misspend of funding. A monitoring visit was undertaken to one provider and overpayment identified and clawed back.

9. Savings

Savings associated with special investigations and counter fraud work are difficult to quantify. Sometimes there will be direct savings, for example stopping a fraud at source, recovery of a duplicate payment or repayment of a dubious transaction, e.g. travel or overtime claim, whereas other savings from the counter fraud function is unquantifiable, e.g. the notional 'value' associated with ongoing proactive counter fraud work and fraud awareness

raising, and other 'deterrence' activity. In practice, however, it is not possible to gauge or calculate how many frauds or errors have been prevented as a result of fraud advice, fraud awareness raising and promoting a strong internal control environment.

Examples of savings made include the repayment of an overclaim by a provider (c. £3k), repayment of ineligible expenditure incurred (c. £870), the prevention of a salary misdirection (c. £4k) and the blocking of a fraudulent grant applicant, thus preventing bogus claims from coming in.

For initiatives such as the National Fraud Initiative (see para. 20) there is a nationally accepted formulae set used to extrapolate and put an estimated 'educated guess' value to savings. As an example, if an overpayment is identified to a deceased person (e.g. pension), the formula assumes that, if it had not been detected, the overpayment would have continued until that individual's 80th birthday.

10. Lessons Learned / Continued Service Improvement

Despite best efforts to mitigate fraud risk it is inevitable that within a large organisation such as the County Council there will be fraudulent activity from time-to-time. Part of the Council's response to fraud is a review of lessons learned, in conjunction with the relevant service concerned, and subsequent process improvements in order to prevent or mitigate the risk of recurrence. Any actions arising from this activity may be included in the Council's Counter Fraud Action Plan where appropriate.

11. Governance of Counter Fraud Activity

Oversight of counter fraud activity rests with the Head of Internal Audit & Assurance Service and the Assistant Director – Strategic Finance & Commissioning, both of whom receive regular updates on counter fraud work and ongoing investigations.

Counter fraud updates are provided to each meeting of the Corporate Governance Committee as part of the standing risk management update

and it is intended to maintain an Annual Counter Fraud Report to the Committee.

12. International Fraud Awareness Week (IFAW)

The Internal Audit & Assurance Service uses IFAW, in November each year, to issue targeted messages to staff during the week via the Intranet and other means on a range of topical fraud risk areas. A strong and continuous process of raising awareness of fraud risk with staff remains a key defence against fraud and IFAW provides an ideal opportunity each year to convey important messages through proactive communications. This also includes advice to staff on fraud risks in their personal lives as part of our 'good employer' obligations.

Whilst IFAW gives a good opportunity to specifically focus on counter fraud awareness raising and other initiatives, in reality proactive counter fraud

work takes place throughout the year, with ongoing advice and support provided within the organisation at relevant points.

Additionally, colleagues within ICT Services used Cyber Security Awareness Month in October 2024 to raise awareness of cyber security and its profound impact on everyone's personal and professional lives. There is often a link between fraudulent activity and cyber-crime, including phishing, spoofing, QR-code fraud ('quishing') and identity theft, although cyber-crime has a broader spectrum wider than just fraud, e.g. denial of service attacks, ransomware, software piracy, cyber-bullying, on-line money laundering.

13. Fraud Risk Assessment

The CIPFA Code of Practice – 'Managing the Risk of Fraud & Corruption' recommends that local authorities identify and assess the major risks of fraud and corruption to the organisation. The Internal Audit & Assurance Service performs a biennial fraud risk assessment and uses the results to direct counter fraud resources accordingly. The County Council does not provide some of the services that have traditionally been considered to be at high risk of fraud, such as revenue and benefits but it is recognised that the Council cannot become complacent regarding the risk of fraud and its effect on the public purse.

National fraud intelligence received through networks such as the CIPFA Counter Fraud Centre and the National Anti-Fraud Network (NAFN) helps to inform local authorities of key current fraud risks for councils and also of emerging frauds relevant to the sector. Such intelligence is used proactively to inform the fraud risk assessment. The Council networks closely with other local authorities to share both fraud intelligence and strategies to manage fraud risks, including via the Midland Counties' Fraud Group.

The highest-scoring areas in the Council's Fraud Risk Assessment (2024) are procurement fraud (both pre-contract award stage and post-contract award stage), social care fraud (e.g. misuse of direct payments, deprivation of assets to increase the Council's contribution to care costs), cybercrime, mandate fraud and insider fraud. These high-scoring areas are typically those reported nationally by other councils too. The fraud risk assessment

helps to direct the Council's overall strategy for countering fraud and enables the Council to direct its counter fraud resources accordingly. Consequently, this informs the internal audit annual planning process where a range of audit assignments will typically be developed within the annual audit plan with specific fraud risks in mind.

In terms of *emerging* fraud risks, cyber-crime becomes ever more sophisticated, whilst the risks associated with insider fraud are acknowledged as being greater during economic downturn, e.g. with cost-of-living pressures.

In terms of *decreasing* fraud risks, cash frauds and thefts are less prominent as we move increasingly to becoming a cashless society, with electronic transactions becoming increasingly the norm. It should be noted however that electronic payments bring specific risk too, e.g. cyber-enabled fraud and this simply demonstrates the need to recognise that those involved in fraudulent activities will adapt their methodology to achieve their objectives.

There is no such thing as 'a typical fraudster'. Whilst many fraudsters are organised career criminals, skilled in the art of deception, often based overseas, other fraudsters are simply 'chancers', taking the opportunity to commit fraud due to personal circumstances (motivation) or simply because the opportunity to defraud arises, e.g. insider (employee) fraud.

The 'Fraud Triangle' [Cressey] illustrates the three fundamental factors that contribute to the risk/likelihood of fraud – (i) opportunity, (ii) rationalisation and (iii) pressure (motivation). Through effective internal controls, organisations such as the County Council can significantly reduce the opportunity for somebody to commit fraud, whilst continued fraud awareness raising can manage the rationalisation factor by imparting a strong message that fraud committed against a large organisation such as the County Council is not a victimless crime and that every pound lost to fraud is a pound that could have otherwise been spent on essential public services.

14. Insider (Employee) Fraud

Within any large organisation there is the risk of insider, or employee, fraud. Insider fraud can take many forms including, but not restricted to, theft of cash or assets, bribery and corruption (e.g. undeclared conflicts of interest), concealed nepotism, recruitment fraud, sickness absence fraud, secondary employment (specifically being absent in one job in order to undertake another), funds re-diversion to false bank accounts, misuse of assets (e.g. vehicles), expenses fraud (e.g. overtime, expense claims), abuse of position, theft of information.

The Council seeks to manage the risks associated with insider fraud through a number of ways including having robust policies and procedures in place (e.g. Employee Code of Conduct), effective corporate induction processes, staff mandatory fraud training, a strong internal control environment and a robust deterrence through our published zero-tolerance approach to fraud and financial irregularity.

The Council operates robust recruitment / on-boarding processes designed to ensure that candidates are both bona fide and suitable for employment within the organisation, including DBS checking, validation of qualifications and/or professional registrations, following-up gaps in employment history and the taking-up of references, e.g. from previous employment.

15. Failure to Prevent Fraud

A new offence of 'failure to prevent fraud' will come into force on 1 September 2025, after having been introduced by the Economic Crime and Corporate Transparency Act 2023. The legislation has created this new failure to prevent fraud corporate offence to hold organisations to account if they profit from fraud committed by their employees or other "associated persons" working on behalf of the organisation.

Since the Council is within the scope of the legislation, an internal risk assessment has been undertaken which identifies that there is low risk to the Council due to the nature of its operations. The offence arises only where employee fraud directly benefits the organisation itself so is more geared to commercial sectors such as sales, e.g. corrupt sales practices leading to increased profits for the organisation concerned.

It is a defence for an organisation to show it has "reasonable procedures" in place to prevent fraud at the time that the fraud was committed. Early steps have been taken to catalogue the wide range of counter fraud controls in place within the Council to mitigate the risk of employee (insider) fraud or fraud by other "associated persons". These include mandatory fraud awareness training, a defined and updated declaration process for conflicts of interests and for gifts and hospitality, a formal whistleblowing channel, fraud referral channels and the operation across the Council of a robust internal control environment.

16. Counter Fraud Action Plan

A two-yearly counter fraud action plan is in place setting out several key actions / improvements intended in the medium-term to improve the Council's resilience to fraud risk yet further. The current action plan (2024-26) is shown towards the end of this report (Appendix 1).

Oversight of the action plan is provided by the Head of Internal Audit & Assurance Service and the Assistant Director – Finance, Strategic Property & Commissioning, both of whom receive regular progress updates regarding

the implementation of intended actions, and by the Corporate Governance Committee which receives updates on the status of the action plan.

17. Counter Fraud Policies and Procedures

The Internal Audit & Assurance Service is responsible for the maintenance of the Council's counter fraud policies – the overarching Anti-Fraud & Corruption Strategy, and supplementary policies on Anti-Bribery, Money Laundering and Preventing the Facilitation of Tax Evasion. These complement other council polices, indirectly fraud-related, such as Gifts & Hospitality, Pecuniary & Business Interests, Employee & Member Codes of Conduct and Whistleblowing.

These policies can be accessed on the Council's website as well as, internally, on the corporate intranet - Fraud | Leicestershire County Council

The four policies produced by the Internal Audit & Assurance Service have been revised during the 2024/25 financial year as part of a standard two-yearly review and update process.

18. Fraud Referral Channels

During the 2024/25 financial year two new avenues have been developed to enable both staff and the general public to raise fraud concerns with the Council. These are (i) a generic fraud email mailbox, and (ii) a web-based e-referral form. The existence of these new channels of reporting fraud has been promoted to staff through several channels including internal communications, e-learning tools and a noticeboard poster campaign.

On a small number of occasions, incoming fraud referrals are noted to **not** have relevance to the County Council, e.g. benefit fraud (DWP), income tax avoidance (HMRC) or council tax fraud (district colleagues). Also, on occasions, referrals are received that should have been made to Leicester City Council. In such instances our approach is to forward on the referral to the appropriate council / agency.

19. Data Matching

The Council is an active participant in the National Fraud Initiative (NFI). The NFI is a mandatory data-matching exercise coordinated by the Cabinet Office which seeks to identify potential anomalies and fraud through matching the Council's data sets, e.g. payroll, pensions, creditors, employee data (potential conflicts of interest), blue badges, concessionary travel, etc., with those of other mandatory participants, including the Department for Work and Pensions deceased persons data and company director data held at Companies House.

Examples of what NFI data matching might identify include:

- Continuing payment of pension to a deceased person.
- An employee with a job at another organisation concurrent to his/her employment with LCC.
- An employee and a creditor with the same bank account, i.e. undeclared connections and potential corruption.
- Other undeclared personal interests, e.g. company directorships.
- Duplicate payments.
- Continuing service provision where a person is deceased, e.g. a disabled parking pass (blue badge) remaining in circulation with an associated risk of third-party misuse.

The Internal Audit & Assurance Service also undertakes internal data matching through bespoke products intended to identify fraud or error, e.g. duplicate payments analysis, or undisclosed employee relationships to suppliers, e.g. through matching employee to creditor bank accounts.

20. National Fraud Initiative 2024-26

Output from the latest NFI exercise (2024-26) was released back to Councils in December 2024. Work is currently underway to review matches to determine if there are instances of fraud or error. A summary of the output from NFI 2024-26 is appended at Appendix 2.

Outcomes will be reported through to the Corporate Governance Committee at the conclusion of the exercise.

21. Reporting Fraud under the Local Government Transparency Code

Under the statutory Local Government Transparency Code 2015 (updated in January 2025), the Council is required to publish on its website, annually, summary details of fraud investigations including the total number of frauds investigated and the total amount spent by the authority on the investigation of fraud. Details for 2024/25 have been published and can be viewed via the link below: -

https://www.leicestershire.gov.uk/about-the-council/council-spending/payments-and-accounts/cost-of-fraud-investigations

22. Whistleblowing

The Council's whistleblowing process is administered by the Director of Law & Governance and Director of Corporate Resources. Whistleblowing referrals to the Council arise on a wide range of issues, including regarding fraud or financial irregularity. Where a whistleblowing referral concerns fraud, the standard process is for it to be referred to the Head of Internal Audit & Assurance Service and progressed under the Fraud Response Plan.

In addition, the Director of Law & Governance and Director of Corporate Resources take an annual whistleblowing report to the Corporate Governance Committee.

23. Mandatory Fraud Awareness Training

The Council's mandatory fraud awareness training module was refreshed during the 2024/25 financial year. As part of this refresh, all staff will be expected to undertake recertification within an initial six-month period.

At the end of the financial year, the take-up rate had reached 65%. As the initial six-month completion window draws to a close, steps will commence to identify and specifically target individual sections where take-up is low.

Furthermore, two-yearly refresher training on fraud awareness has been developed in an on-going effort to keep fraud risks prominent in the minds of staff. This refresher training is mandatory for all staff. Historically, fraud awareness training required 'one-off' completion only and this refresher training will should help to keep fraud risk at the forefront of everybody's minds and mitigate the risk of staff fraud awareness knowledge waning over time.

Additional training exists specifically regarding procurement fraud risk and efforts continue to promote this training to those staff with elements of procurement activity within their job roles and responsibilities.

During the last year, the Council's fraud resource page on the Corporate Intranet (SharePoint) has been refreshed. This page contains advice and guidance to staff on a range of fraud-related issues.

24. Links With Other Internal Services

As well as being the contact point for departments with regard to fraud-based concerns, the Internal Audit & Assurance Service works with internal services with regard to fraud prevention advice and other proactive counter fraud communications. This includes close working with Legal Services, Human Resources, ICT Services, Trading Standards and the Corporate Communications Team.

The Council's Trading Standards Scams Team issues advice to consumers through the year through consumer newsletters, social media presence and other communications, e.g. Leicestershire Matters. The Council is well-placed to help consumers and the general public to become and remain 'fraud aware' and to develop a scepticism that sometimes all is not what it seems.

25. Liaison with Leicestershire Police

The Council's Fraud Response Plan includes discussion with Legal Services including consideration of referral to the police to consider whether criminal investigation is appropriate depending on the circumstances.

The Council has forged links with Leicestershire Police and has a named contact within the Force's Economic Crime Unit. This enables developing

investigations to be discussed with the Police at an early stage and, if relevant to do so, prior to formal referral as a crime.

26. External Networking

The Internal Audit & Assurance Service networks with external bodies and organisations to share fraud intelligence and advice. This includes the Midland Counties' Fraud Group, the CIPFA Counter Fraud Centre, The National Anti-Fraud Network (NAFN), The East Midlands' Cyber Resilience Centre, neighbouring Leicester City Council's Corporate Fraud Investigations Team, The National Trading Standards Service, The Cabinet Office, and Leicestershire Police.

27. Other Fraud-Related Work Across the Council

Supplementary to the counter fraud work discussed in this report and largely co-ordinated by the Internal Audit & Assurance Service, there is other business-as-usual work within the Council which could have a fraud slant, for example: -

- Disabled person's parking permits (blue badges), where (district council employed) Enforcement Officers will issue Penalty Charge Notices (PCNs) in cases of low-level blue badge misuse.
- Leicestershire Registration Service, e.g. sham marriages or concerns surrounding impersonation and identity crime.
- Trading Standards enforcement work, e.g. counterfeit goods, rogue trading, other business-specific fraud.
- Adult Social Care – assessment of care needs, financial assessment, validity of spend, e.g. personal budgets.

28. Schools and Colleges

Maintained schools operate with a significant degree of independence from the Council. Nevertheless, the Internal Audit & Assurance Service issues proactive counter fraud advice to schools, e.g. dissemination of intelligence about new and emerging fraud threats for schools through the Schools' Portal, or best practice advice.

The Internal Audit & Assurance Service undertakes routine assurance audit visits on a risk-assessed basis to maintained schools. Audit coverage during visits assesses that schools have effective controls in place to safeguard against fraud, an example being a separation of duties in key financial processes (e.g. ordering and payments). Where vulnerabilities are identified that give rise to fraud risk, these are escalated to governing bodies in a written report.

Appendix 1 – Counter Fraud Action Plan 2024-26

#	Action	Target Date
1.	Biennial revisions to the (four) counter fraud policies that are owned by the Internal Audit & Assurance Service (Anti-Fraud & Corruption Policy, Anti-Bribery Policy, Policy for the Prevention of Facilitation of Tax Evasion, Anti-Money Laundering Policy). To include a rationalisation by size of the Anti-Fraud & Corruption Policy.	October 2024
2.	Issue targeted comms to key staff and departments during International Fraud Awareness Week (November each year) highlighting key fraud risk areas.	November 2024 and 2025
3.	Biennial refresh of the Council's Fraud Risk Assessment.	January 2025
4.	Explore and develop mandatory refresher training to supplement the corporate e-learning module on fraud awareness.	April 2025
5.	Consider, in conjunction with the Director of Law & Governance and s.151 officer, the development of both an on-line fraud referral e-form on the Council's website, and a generic fraud mailbox.	April 2025
6.	Develop the concept of there being a corporate risk of fraud and having this risk scored for potential inclusion on the corporate risk register, to formalise the risk itself and the mitigation strategies both in place and proposed.	April 2025
7.	To co-ordinate investigations into priority matches identified by the National Fraud Initiative 2024/25 output reports.	August 2025

8.	Explore the virtues of developing a role of a departmental fraud champion, a friendly face within each department who can act as a point of initial contact for both departmental staff and the corporate counter fraud function, e.g. dissemination of information.	August 2025
9.	Evaluation of additional services available to procure through the National Fraud Initiative (NFI), CIFAS, and other solutions, e.g. additional data matching, supplementary to the main (two-yearly) NFI exercise.	August 2025
10.	Evaluate the potential benefits of moving to an annual counter fraud report to the Corporate Governance Committee.	August 2025
11.	To deliver fraud awareness training to School Business Managers through the (new) SBM Forum established by the C&FS department (c/f from 2022-24 Action Plan due to department inactivity).	December 2025
12.	Monitor changes and enhancements to the Council's processes regarding blue badge fraud resilience post the outcome of the Department for Transport (DfT) national review of blue badge fraud and councils' approaches to tackling it (c/f from 2022-24 Action Plan due to DfT inactivity).	December 2025
13. NEW	Roll-out within the Council of the Fighting Fraud & Corruption Locally (FFCL) Adult Social Care fraud toolkit and resources.	July 2025
14. NEW	Contribute to the Transformation Unit's work on Savings Under Development – Direct Payments.	July 2025
15. NEW	To review the process for identifying and actioning any lessons learned following closed investigations.	July 2025

Appendix 2 – Summary of NFI Output 2024-26

NFI Report Ref. No.	Description	See Note	Number of Matches
52	Pensions to DWP Deceased	2	169
54-57	Pensions to Payroll		619
66-67	Payroll to Payroll	1	35
78	Payroll to Pensions	1	3
80-81	Payroll to Creditors	1	51
170-173	Blue Badge Parking Permit to Blue Badge Parking Permit		322
172.1	Blue Badge Parking Permit to DWP Deceased	3	1215
172.2	Concessionary Travel Permit to DWP Deceased	3	5533
172.3	Residents Parking Permit to DWP Deceased	3	1
175.6	Residential Parking Permit – same vehicle registration		4
303	Blue Badges to Amberhill Data	5	2
306	Concessionary Travel to Amberhill Data	5	1
700-703	Duplicate Creditors	1,4	356
707-713	Duplicate Records	1, 4	9343
709	Overpaid VAT	1	54
750-752	Procurement – Payroll to Companies House	1	34

Notes

(1) Output includes ESPO matches too. ESPO matches are, however, investigated separately and ultimately reported through to ESPO Management Committee.

(2) There is a delay between data being uploaded to NFI and NFI output being received back by participants. Whilst matches to the DWP deceased persons data are always prioritised, e.g. pensions, in most cases, come the time of output being investigation, the deaths have long since been identified though standard business-as-usual processes and relevant action taken.

(3) Due to Blue Badges and Concessionary Travel Permits being issued with a long-term expiry date, it is not uncommon for a permit to still be technically 'in date' despite the permit holder having deceased mid-term. This does not necessarily indicate misuse or fraud although higher-risk outliers are investigated on a risk-assessed basis.

(4) Due to LCC and ESPO being required to submit separate data sets, but which are later consolidated into one output set, this does give rise to false positives on some of the reports, e.g. report 708, where a large number of suppliers who trade with both LCC and ESPO are shown erroneously as potential duplicates. These are discounted at triage stage.

(5) Amberhill is an initiative led by the Metropolitan Police Service. The team collate and distribute data on false identities and share it with counter crime partners, including the NFI, to help detect fraud. This data consists of counterfeit and forged passports, national identity cards and driving licences which are manufactured or obtained by organised criminal gangs. Amberhill data also includes fraudulently obtained genuine UK driving licences.

This page is intentionally left blank