APPENDIX A

Leicestershire County Council

Internal Audit & Assurance Service

Annual Counter Fraud Report (April 2025 – March 2026)

Leicestershire County Council Internal Audit & Assurance Service

Annual Counter Fraud Report (April 2025 – March 2026)

1. Introduction

This report summarises the counter fraud activity that has taken place within the County Council during the 2025/26 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 restricted solely to fraud investigations but extends to other non-fraud related 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.

2. Fraud Landscape

Fraud and error cost the taxpayer billions of pounds each year – but much 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 between £55 billion to £81 billion in 2023-24 (a high majority of the loss being against HMRC and the DWP). Only a fraction of this is detected and known about – enabling investigation and recovery.

The Local Government Transparency Code includes an estimation that the cost of fraud to local government alone 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 to the benefit of local taxpayers. Local authorities continue to

face significant fraud challenges and 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.

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. Looking forward to Local Government Reorganisation, if the Government chooses a future council for Leicestershire & Rutland, this will see exposure to this wider range of fraud risks.

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. Fraud could be perpetrated by a rogue individual(s) or could be the focus of organised crime groups. As a result of fraud and financial crime, organisations experience revenue loss, reputational damage, and increased operational costs.

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.

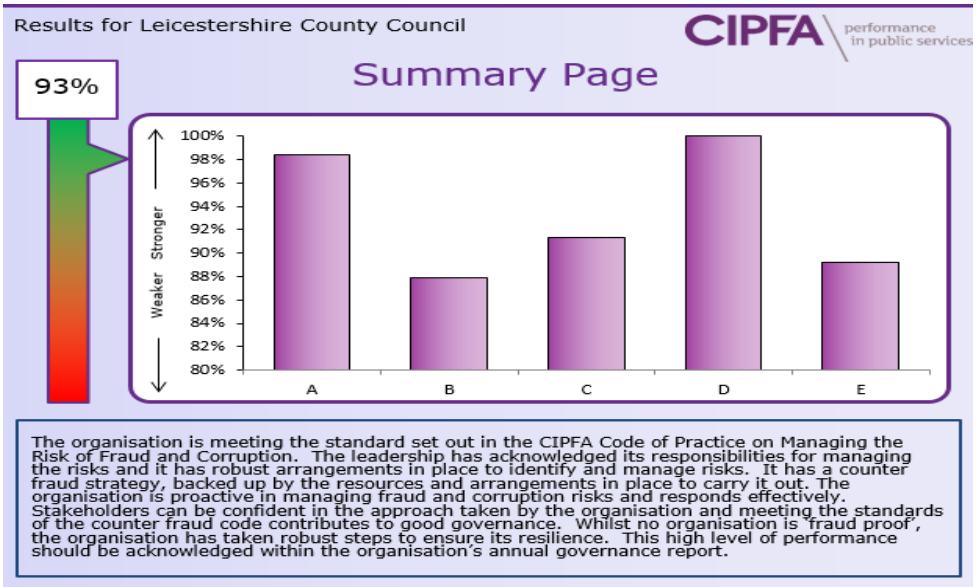
The Council fully recognises its responsibility for spending public money and safeguarding public assets. The prevention, and if necessary, the investigation, of fraud and corruption is therefore seen as an important aspect of its duties which it is committed to undertake.

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. Councils 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:

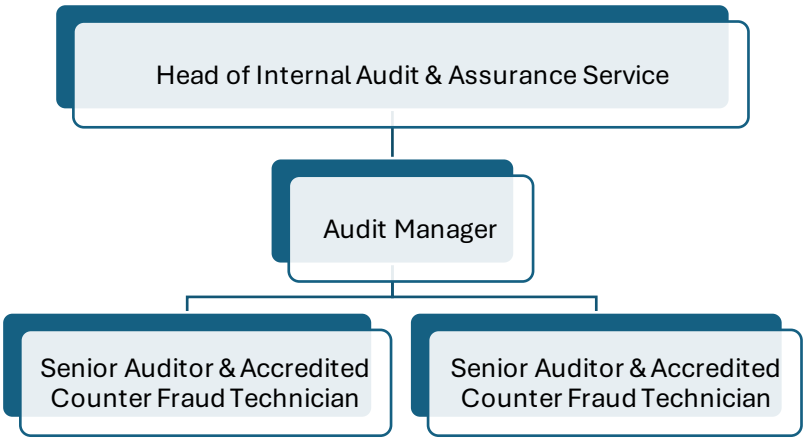
A - Acknowledge the responsibility of the governing body for countering fraud and corruption
B - Identify the fraud and corruption risks
C - Develop an appropriate counter fraud and corruption strategy
D - Provide resources to implement the strategy
E - Take action in response to fraud and corruption.

The most recent assessment was undertaken in 2023. The assessment method is primarily through self-evaluation; however, the Council elected to have its self-assessment peer reviewed by the Corporate Investigation Manager from a neighbouring council to independently stress-test the results/conclusions reached and to give an independent opinion that these were reasonable. The results of the 2023 assessment were overall positive with the recommendations arising from the assessment duly 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 Accredited Counter Fraud Technician (ACFT) 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, referrals coming from the biennial National Fraud Initiative data-matching exercise (NFI)). For the 2025/26 financial year, the total time incurred on counter fraud work was 73 days. The two senior auditors devoted almost 62 days (approximately 20% of their resource net of overheads and work for other clients).

6. Number and Status of New Investigations Commencing in 2025/26

	2025/26		*2024/25 (comparison)*
New Fraud Investigations Commencing in 2025/26 (*)	17	100%	*17*
Number Closed at Year-End	12	71%	*13*
Number Remaining Open at Year-End	5	29%	*4*

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 People Services 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/teams, 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 at an early stage to determine the Police's likely involvement. Occasionally, internal investigations will run parallel to Police investigations bringing potential complexity that may require careful coordination and management.

8. Summary of Investigations Closed in 2025/26 by Age

2025/26 Investigations Closed During 2025/26	12
Prior Year Investigations Closed During 2025/26	8
TOTAL NUMBER CLOSED DURING 2025/26	20

A summary of themes in relation to common fraud risks and investigations undertaken includes the following (n.b. this captures *closed* investigations only; it would not be appropriate at this stage to discuss details of *ongoing* investigations):

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.
Council funding of external providers	This can comprise false or exaggerated claims or misspend of funding. In one case an overpayment was identified and clawed back, not due to fraud but due to a setting closing down unexpectedly.
Social Care	Social care fraud can include direct payments fraud, deprivation / non-declaration of assets and financial abuse of vulnerable service users (safeguarding). An investigation was undertaken following an incoming fraud referral. The case was noted to be 100% health funded so the investigation was passported to NHS Fraud after initial triage by the Council. Another investigation into the alleged theft of a service user's funds led to a successful Police prosecution. In a further case, a service user's contributions to the cost of care were reassessed following an investigation into concealed assets.
Disabled Parking Permits (Blue Badges)	Output from the National Fraud Initiative highlighted one case where a blue badge application was seemingly made after the individual's date of death. The blue badge was duly cancelled.
Insurance Fraud	Insurance fraud can take many guises, most commonly false or exaggerated claims. An investigation into a suspected exaggerated claim led to the insurance claim being rejected and the case reported to the Police.
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.
Schools	Schools have delegated responsibility for finance. Loss recovery advice was given to a school that incurred a small financial loss as a result of mandate fraud.
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.
Grants Payable	Grant fraud can comprise bogus or exaggerated applications or misspend of grant. An incoming fraud referral led to an investigation into a community group, but it was determined that the group was not County Council-funded but instead grant funded by a Leicestershire District Council. The referral was duly passported on to the appropriate council.
Concessionary Travel	Allegations received regarding the alleged misuse of a personal transport budget (PTB) by a service user were disproven upon investigation. Whilst the referral was made to us in good faith, the referrer has misunderstood the PTB rules and there was no actual misuse.

9. Financial Outcomes / Recoverables

Financial outcomes associated with special investigations and counter fraud work are difficult to quantify. Sometimes there will be direct benefits achieved, 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 benefits arising from the work of the counter fraud function are unquantifiable, e.g. the notional 'value' associated with ongoing proactive counter fraud work and fraud awareness raising, and other 'deterrence' activity. 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 maintaining a strong internal control environment.

Examples of recoverables during the year include the challenge to, and rejection of, an exaggerated insurance claim (c. £10k), the recovery of an advanced payment to a commissioned provider that subsequently ceased to operate (c. £11.5k) and the reassessment of a client's social care financial assessment due to the identification of concealed assets (c. £8.9k).

The National Fraud Initiative (NFI) is a biennial, national, data-matching initiative co-ordinated by the Public Sector Fraud Authority (PSFA). NFI sees the Council's data 'matched' against data from many other mandatory participants with anomalies returned to participants for further investigation. For initiatives such as the National Fraud Initiative there is a nationally accepted formulae set used to extrapolate and put an estimated value to 'forward savings'. Reportable figures reflect that full benefit can be both an *actual amount* recovered and a notional '*forward saving'* (estimation of future loss prevented).

Examples of positive outcomes from National Fraud Initiative (NFI) work include the recovery of payments to a care home failing to notify the Council of the death of a resident (c. £32k), the recovery of a direct payment overpayment as a result of an incorrect date of death held (c. £600) and a notional benefit due to the cancellation of a fraudulently obtained blue badge (c. £800). In addition, because of NFI work a number of both blue badges and concessionary travel passes have been cancelled where the holders have been identified as recently deceased. NFI attributes standard 'financial benefit' figures of £794 (blue badges) and £38 (concessionary travel passes) respectively in each case.

Additionally, internal audit-brokered work through the National Fraud Initiative has identified a small number of not-known-about deaths in relation to the Pension Fund, enabling steps to be undertaken to seek recovery of overpayments made. Whilst deaths are generally identified through business-as-usual channels, NFI work does pick up some deaths earlier in the process thus it brings advantage in minimising the value of any

overpayments that may otherwise be made. This can aid the recovery process.

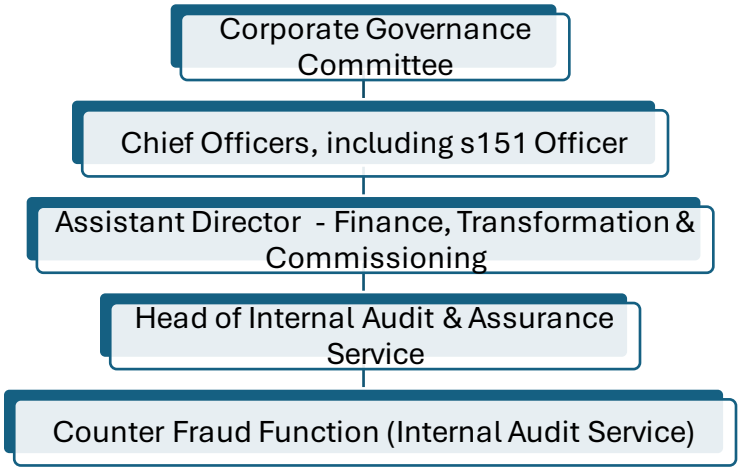
It is not uncommon for the Council to receive fraud referrals in error that are, for example, relevant to district councils, e.g. council tax fraud. These are passported on to the relevant council/agency for action. Such referrals are likely, ultimately, to lead to further savings to the public purse. Misdirected fraud referrals, therefore, are a good example of us sharing intelligence received with other councils/agencies for the wider benefit of the public purse.

10. Lessons Learned / Continued Service Improvement

The Council takes fraud prevention seriously and has effective controls in place, but the scale of the organisation means that some instances may still arise from time to time. Part of our standard response to every fraud is a review of lessons learned, in conjunction with the relevant service concerned, and implementation of process improvements in order to prevent or mitigate the risk of recurrence.

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, Transformation & Commissioning, both of whom receive regular updates on counter fraud work and ongoing investigations.



Counter fraud updates are provided to the Corporate Governance Committee primarily through this annual reporting process as well as ad hoc in-year reporting as part of the standing risk management update, where appropriate.

12. International Fraud Awareness Week (IFAW)

During International Fraud Awareness Week each November, Internal Audit & Assurance delivers targeted fraud awareness messages to staff. The campaign strengthens fraud prevention and includes practical advice on personal fraud risks as part of the Council's good employer responsibilities.

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 as and when relevant.

During IFAW 2025 messages were shared with staff on topics such as career polygamy risk (overemployment), cyber-enabled fraud, declaring secondary employment, how to report concerns, the new corporate 'Failure to Prevent Fraud' offence, mandatory fraud awareness training and common frauds and scams.

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 many 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 counter fraud networks helps to inform 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 Council's latest Fraud Risk Assessment (2024) highlights procurement fraud, social care fraud (e.g. misuse of direct payments, deprivation/concealment of assets), cybercrime, mandate fraud and insider fraud as high-scoring fraud risks. These high-scoring areas are typically those recognised up and down the country 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 risk areas 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. Artificial intelligence (AI) is a major emerging fraud risk globally and an enabler to cyber-crime. Career polygamy too is seen as an emerging fraud risk, i.e. an individual undertaking two or more jobs concurrently.

We are yet to fully see how artificial intelligence (AI) will change the fraud landscape, both as an *enabler* to fraud and a key tool in the *detection* of fraud and error. Organised criminals are adopting generative artificial intelligence (GenAI) tools such as deepfakes, large language models, and voice cloning to improve the sophistication, credibility and volume of attacks, and indeed the ease with which they can be carried out. Criminals are likely tailoring these tools to specific victims and fraud types, making attacks more effective and harder to detect.

We continue to raise the risk of AI-enabled fraud with key services, e.g. recruitment fraud, grant fraud, and continue to horizon scan for opportunities to use AI and other data-driven solutions to identify fraud and/or error.

In terms of *decreasing* fraud risks, cash frauds and thefts are less prominent 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 continually adapt their methodology and tactics as the fraud landscape changes.

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.

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 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 fraud. Insider fraud can take many forms including, but not restricted to, theft of cash or assets, bribery and corruption, concealed nepotism, recruitment fraud, sickness absence fraud, undeclared secondary employment, funds re-diversion to false bank accounts, misuse of assets (e.g. vehicles), expenses fraud, 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 and firm sanctions where fraud or financial irregularity is apparent.

The Council operates robust recruitment / on-boarding processes designed to ensure that candidates are both bona fide and suitable for employment within the organisation.

15. Failure to Prevent Fraud

A new corporate offence of 'failure to prevent fraud' came into force on 1 September 2025, after having been introduced by the Economic Crime and Corporate Transparency Act 2023. The legislation has created the new 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 considers that there is low risk to the Council due to the nature of its operations. The offence arises only where employee fraud *benefits* the organisation itself.

It is a defence to the corporate offence for an organisation to show it has "reasonable procedures" in place to prevent fraud at the time that the fraud was committed. 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", e.g. agency staff, consultants, contractors, service providers.

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 at Appendix 1.

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

the implementation of intended actions, and by the Corporate Governance Committee which receives periodic 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, which are owned by the Chief Legal Officer (Monitoring Officer).

These fraud policies can be accessed on the Council's website as well as, internally, on the corporate intranet.

18. Fraud Referral Channels

During the previous (2024/25) financial year two new avenues were 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 channels of reporting fraud is promoted to staff through internal communications, e-learning tools and a noticeboard poster campaign.

On 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/unitary councils). In any 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 Public Sector Fraud Authority (PSFA), a function of the Cabinet Office, which seeks to identify potential anomalies and fraud through matching the Council's data sets, e.g. payroll, pensions, creditors, adult social care, etc.

Examples of what NFI data matching might identify include:

- Continuing payment of pension to a deceased person.
- Continued payments for social care provision 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) or a concessionary travel pass remaining in circulation with an associated risk of third-party misuse.

The Internal Audit & Assurance Service also periodically undertakes internal data matching using data analysis tools 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

The National Fraud Initiative (NFI) is a country-wide data matching exercise that takes place every two years. The Council is a mandatory participant. Output from the latest NFI exercise (2024-26) was released back to councils and other participants in December 2024 and investigations are complete.

21. Reporting Fraud under the Local Government Transparency Code

Under the statutory Local Government Transparency Code 2015, 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: -

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 Chief Legal Officer (Monitoring Officer) and Director of Corporate Resources. Whistleblowing referrals to the Council can arise on a wide range of issues, including regarding fraud or financial irregularity. Where a whistleblowing referral concerns fraud it is progressed under the Fraud Response Plan.

In addition, the Chief Legal Officer 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 is available to all staff, both digitally and in manual formats. Take-up is currently over 88%, commensurate with the Council's other mandatory training modules. Steps continue to target those sections with low take-up rates.

Two-yearly mandatory refresher training on fraud awareness has been developed in an on-going effort to keep fraud risks prominent in the minds of staff.

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.

The Council's fraud resource page on the Corporate Intranet (SharePoint) is maintained up-to-date and remains relevant. This page contains advice and guidance to staff on a range of fraud-related issues and links to relevant policies and fraud referral channels.

24. Links With Other Internal Services

As well as being the contact point for departments with regards 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 the Chief Legal Officer (Monitoring Officer), Legal Services, People Services, ICT Services, Trading Standards and the Corporate Communications Team.

Fraud alerts are issued to key stakeholders throughout the year, e.g. based on national intelligence received (and other sources). These can be via a variety of means, e.g. corporate intranet, direct contact, etc.

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 a criminal investigation is appropriate depending on the circumstances.

The Council has strong links with Leicestershire Police and in particular with the Force's Economic Crime Unit. This enables developing investigations to be discussed with the Police at an early stage and, if necessary, 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 local authorities, The National Trading Standards Service, The Cabinet Office, and Leicestershire Police.

27. Other Fraud-Related Work Across the Council

In addition to specific counter fraud work, there is business-as-usual work within the Council which has a fraud slant, for example: -

- Disabled person's parking permits (blue badges), where 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.
- Social Care – assessment of care needs, financial assessment, validity of spend, e.g. direct payments.
- Welfare grant funding, e.g. Crisis & Resilience Fund.
- Procurement, both at pre-contract and post-contract award stages.

28. Schools

Maintained schools operate with a significant degree of autonomy 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. Specific fraud advice was issued to schools during International Fraud Awareness Week 2025.

The Internal Audit & Assurance Service undertakes routine assurance audit work in schools, predominantly through themed audits, whilst we reserve the right to undertake site visits, unannounced if required, where there are specific concerns arising.

Appendix 1 – Counter Fraud Action Plan 2024-26

#	Action	Target Date	Status
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	Complete
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	Complete
3.	Biennial refresh of the Council's Fraud Risk Assessment.	January 2025	Complete
4.	Explore and develop mandatory refresher training to supplement the corporate e-learning module on fraud awareness.	April 2025	Complete
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	Complete
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	Ongoing

7.	To co-ordinate investigations into priority matches identified by the National Fraud Initiative 2024/25 output reports.	August 2025	Complete
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	Complete
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	Complete
10.	Evaluate the potential benefits of moving to an annual counter fraud report to the Corporate Governance Committee.	August 2025	Complete
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 resource issues).	December 2025	Delayed but replaced by written fraud advice to schools
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	Ongoing

13.	Roll-out within the Council of the Fighting Fraud & Corruption Locally (FFCL) Adult Social Care fraud toolkit and resources.	July 2025	Complete
14.	Contribute to the Transformation Unit's work on Savings Under Development – Responsible Payments.	July 2025	Ongoing
15.	To review the process for identifying and actioning any lessons learned following closed investigations.	July 2025	Complete

This page is intentionally left blank