Appendix 1

Annual Counter Fraud Report 2024/25

1. Introduction – National Context and Council Policy

The Chartered Institute of Public Finance and Accountancy (CIPFA) estimates that up to £49bn of public money is lost each year as a result of fraud. Of this total, an estimated £8.8bn is specifically located within local government.

It is against this background that in response to the risks and threats presented to the Council by fraud, the Council has in place a Fraud and Corruption Prevention Policy. By way of this policy, the Council acknowledges the significant negative impact fraudulent and corrupt acts can have on the Council, the delivery of its Corporate Plan and the services provided to residents. The Policy also makes clear that the Council takes a zero-tolerance approach to fraud and corruption; will take all necessary steps to prevent, detect and punish fraudulent and corrupt acts; and will take all appropriate action against perpetrator(s) and pursue all available options to recover any losses.

The policy establishes two key processes for the prevention of Fraud and Corruption within the Council. Firstly, the policy outlines (in tandem with the Council's Whistleblowing Policy) a procedure for the reporting of suspected fraudulent and corrupt acts. Such reports are considered by senior management, with the potential for further investigation by Internal Audit, referral to specialist fraud investigation services and/or the Police.

The second key process established by the Policy is an ongoing programme of preventative measures established by relevant departments across the Council, supported by ongoing assurance and advisory work performed by Internal Audit. The basis for this programme is the Fraud Risk Register (presented in Appendix 2) which is maintained by Internal Audit and periodically reviewed in conjunction with relevant Assistant Directors, Heads of Service and other service managers.

A summary of the key measures and activity in each relevant department now follows.

2. Summary of Key Measures and Activity

Revenues and Benefits

As part of the ordinary course of operations, documentary evidence for all claims for discounts, reliefs or benefits are required before any such discount, relief or benefit is awarded. Regular inspection work is also carried out.

The Council participates in a regular Single Person Discount data matching programme provided by the National Fraud Initiative. In addition, much of the current counter fraud activity within the Revenues and Benefits teams is in support of the Department for Work and Pensions (DWP). In 2024/25 this activity included issuing 14 fraud referrals to the DWP and completing 22 Local

Authority Information Exchange Forms (LAIEF) (being requests for information from the DWP to support their ongoing investigations).

Housing

Nationally, the risk of fraud relating to housing has been identified as high value. In a local context, the risks for this Council include the potential for tenancy fraud, sub-letting and risks associated with the 'Right to Buy'.

With regard to tenancy fraud the risks are that an applicant will make false claims on their application to increase their banding, omit information from their application which could demonstrate that they are not eligible or make false statements which could both impact banding and eligibility. To mitigate this, all applicants are asked to provide evidence to support their application, references are taken and records are checked.

All Housing employees are expected to report any concerns regarding sub-letting which will be fully investigated. The Housing Service has also run an awareness raising campaign, informing tenants of the action that can be taken if they sublet and also reminding neighbours of how concerns can be reported.

In respect of 'Right to Buy' applications, appropriate checks are undertaken to prevent and detect potential fraud, including:

- Requesting identity and proof of address for each applicant.
- Checking if the applicant is in receipt of Housing Benefit and referring this on for enquiry (particularly where the sale is expected to be financed without a mortgage).
- Checking each applicant's details with appropriate agencies (including the National Anti-Fraud Network) to see if the applicant has other mortgages and to check the persons registered at the address from electoral records.
- Requiring applicants to provide details as to how they intend to finance the purchase. If monies are being gifted, the Council will require the applicant to provide confirmation from the third party that these funds are available and seek proof of identification.

Procurement

The Council has formal Financial Regulations in place which provide considerable detail into the processes and procedures required in order to complete procurement exercises, including formal tenders. Contract opportunities are well-advertised, with a commonly-used online tendering system being utilised to help ensure transparency and fairness. The Council is also being supported with its procurement activity by the Nottinghamshire County Council Procurement team.

Payroll and Human Resources

All new employees and changes to employee details are subject to robust checking processes which involve, as required, documentary evidence and/or direct confirmation of details with the relevant employee. Areas such as probation, sickness absence, right-to-work and payroll data are similarly supported by established Council policy and documentary checks as required.

Finance Services

The Finance Services team engages with banks and other financial institutions to prevent fraudulent activity. This includes both treasury management activity and creditors payments to validate bank accounts. Barclays Bank, who provide the Council's banking services, regularly provides officers with fraud awareness briefings and email updates on developments and trends in fraudulent activity.

Environmental Health and Licensing

The Environmental Health team ensures that, where necessary, the identity and relevant details for applicants or premises owners are established and supported by documentary evidence. Reference is made to the National Anti-Fraud Network as required, in addition to cross-agency data sharing and checking.

In addition, the Licensing service continues to check right-to-work status for all new taxi and private hire drivers and for relevant alcohol licensing applications, while all drivers, operators and scrap metal dealers are required to provide proof that they are registered to pay tax on their earnings. These measures assist in preventing illegal working, unlawful employment of workers and unlawful payments to employees.

Insurance

The Council continues to work with its insurers who regularly provide briefings and advice to enable officers to remain vigilant to potential fraudulent claims. All claims continue to be rigorously reviewed at every stage to ensure that anything suspicious is identified and the appropriate outcome is achieved. Claimants are advised that information provided may be shared by the insurers with other appropriate bodies responsible for the prevention and detection of fraud, such as the Claims and Underwriting Exchange Register.

Training and Awareness

As part of the mandatory training provided through the Council's online learning platform (Broxtowe Learning Zone), employees are required to complete modules on Cyber Security and the Code of Conduct in addition to a number of Information Management and Security modules. Other specific courses are available for relevant service areas, including modules on Payment Card Security and Serious Organised Crime.

Internal Audit provides periodic general fraud awareness updates to employees in addition to providing more targeted fraud information to relevant officers.

National Fraud Initiative

The Council participates in the Cabinet Office's National Fraud Initiative programme (NFI), which matches electronic data within and between the public and private sector to assist in the prevention and detection of fraud. These include local authorities, police authorities, local probation boards, fire and rescue authorities as well as a number of private sector bodies. The NFI tool is helpful in assisting to identify potential fraud in areas such as council tax, housing benefit, pensions, payroll and housing tenancy.

The Council periodically provides specified sets of data to the Cabinet Office for matching. The data provided can include records relating to council tax, creditors, payroll, electoral register, housing tenants, housing waiting lists, insurance claims and licences. Whilst Internal Audit is the single point of contact for participation in the NFI data matching programme, the process does require the support of the respective service managers with responsibilities for the service/system being subjected to review under the scheme. A network has been established to enable departments to support Internal Audit with this work.

The latest NFI data matching exercise was performed in January 2025 with 1,687 matches being generated for further review. Upon release of the matches, Internal Audit completed a risk analysis (categorising the matches as 'high', 'medium' and 'low' priority for further investigation) and subsequently began work, in conjunction with relevant officers in other departments, to investigate and resolve the matches according to level of priority and quality of data available.

Internal Audit

No significant special investigations (beyond those performed as part of the NFI data matching exercise) have been carried out by Internal Audit during 2024/25.

Internal Audit has noted a small number of incidents where unknown third parties have attempted to redirect valid payments through false requests to change supplier bank details on the Council's financial system. These have taken the form of email requests, letters and telephone calls. Such attempts have been quickly detected and repelled.

As part of the audit of Creditors and Purchasing, undertaken as part of the Internal Audit Plan for 2024/25, the processes in place to maintain the integrity of supplier details held on the Council's system were reviewed and no issues were noted.

Internal Audit also recently complied and presented to the Council's General Management Team the Annual Assessment of Fraud Risk and Mitigation Report. This report, taking the form of a maturity model, is based upon the self-assessment by Assistant Directors, Heads of Service and other managers of the level of fraud risk within their departments. The focus is on internal / employee-based fraud and covers matters such as annual leave, use of corporate purchase cards and the completion of appropriate training.

3. Plans for 2025/26

The primary focus for the next 12 to 18 months will be the review of the results of the NFI data matching exercise noted above. In addition, the review of system access controls will be considered as a component of all scheduled Internal Audit reviews of Key Financial Systems.

Appendix 2

Fraud and Corruption Risk Register – September 2025

1. Introduction and Background

Compliance with the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption is widely recognised as a key component of a quality governance framework. One of the key principles of the Code is to identify the fraud and corruption risks within an organisation; understand the exposure to these risks and routinely consider these as part of risk management arrangements.

The preparation of the Council's Fraud and Corruption Risk Register, presented in this appendix, satisfies this key principle of the Code. The Fraud and Corruption Risk Register is maintained by Internal Audit and periodically reviewed in conjunction with relevant Heads of Service and other managers. The register is also considered by the General Management Team and will be continue to be presented to this Committee alongside the Annual Counter Fraud Report.

2. Fraud Risk Assessment Matrix

The corporate 5x5 risk matrix is used for assessing the threats for each fraud risk in terms of both the likelihood and impact. A score is provided for both the inherent risk and the assessed residual risk. This matrix reflects the direction of travel in terms of the effect of mitigation measures implemented to help manage a particular risk. It also assists in directing resources to areas where they will have the most influence.

	Risk – Threats					
Likelihood	Almost Certain - 5	**5**	**10**	**15**	**20**	**25**
	Likely – 4	**4**	**8**	**12**	**16**	**20**
	Possible - 3	**3**	**6**	**9**	**12**	**15**
	Unlikely - 2	**2**	**4**	**6**	**8**	**10**
	Rare – 1	**1**	**2**	**3**	**4**	**5**
		Insignificant – 1	Minor – 2	Moderate – 3	Major – 4	Catastrophic – 5
		Impact				

Risk Rating	Value	Action
Red Risk	25	Immediate action to prevent serious threat to provision and/or achievement of key services or duties
	15 to 20	Key risks which may potentially affect the provision of key services or duties
Amber Risk	12	Important risks which may potentially affect the provision of key services or duties
	8 to 10	Monitor as necessary being less important but still could have a serious effect on the provision of key services
	5 to 6	Monitor as necessary to ensure risk is properly managed
Green Risk	1 to 4	No strategic action necessary

In applying the matrix to the fraud and corruption risks posed to the Council, appropriate reference has been made to published guidance and reports from CIPFA, the National Fraud Initiative, Central Government, the external auditors and other relevant organisations. Existing knowledge of the Council's operations derived from previous counter fraud and Internal Audit work has also been drawn upon as appropriate.

This risk register will serve as a 'living document' and evolve over time as the nature of the services provided by the Council and the environment within which it operates changes, giving rise to variations in the Council's risk profile.

Fraud and Corruption Risk Register

Risk Area	Risk	Mitigation	Inherent Score	Residual Score
Housing Tenancy (Applications)	Fraudulent applications for new or successive tenancies	Documentary evidential requirements Checking, review and authorisation procedures Data-matching exercises through NFI	12	6
Housing Tenancy (Subletting)	Sub-letting of Housing properties	Direct and indirect monitoring of tenanted properties Data-matching exercises through NFI Employee training Awareness raising campaign	12	6
Right to Buy	Fraudulent Right-to-Buy applications	Documentary evidential requirements Checking, review and authorisation procedures Data-matching exercises through NFI	16	4
Benefits	Fraudulent applications for Housing Benefit	Documentary evidential requirements Checking, review and authorisation procedures Data-matching exercises through NFI Risk Based Verification of Claims	10	4
Disabled Facility Grants	Fraudulent applications for new or additional grants	Documentary evidential requirements Officer site visits Checking, review and authorisation procedures	12	3

Risk Area	Risk	Mitigation	Inherent Score	Residual Score
Council Tax	Fraudulent applications for discounts and reliefs, including Single Occupier Discount and Local Council Tax Support	Documentary evidential requirements Checking, review and authorisation procedures Data-matching exercises through NFI	15	4
Business Rates (Discounts/Relief)	Fraudulent applications for discounts and reliefs including Small Business Rate Relief and Charitable Relief	Documentary evidential requirements Checking, review and authorisation procedures Property Inspector visiting properties	12	4
Business Rates (Properties)	Unlisted / Concealed Properties	Officer knowledge of borough development Data-matching exercises through NFI Working with third party company to identify gaps	6	4
Procurement (Contract Awards)	Improper award of contracts due to lack of tendering and/or collusion with or between potential suppliers	Procurement and Commissioning Strategy Nottinghamshire County Council Procurement Team Internal monitoring of supplier spends Publication of Contracts Register Code of Conduct Register of interests, gifts and hospitality Contract Management Training and Guidance	16	8
Procurement (Purchases)	Purchase of items for personal use or profit through resale	Authorisation controls through Civica Financials Purchasing and Creditors systems Monitoring of Purchase Card transactions Inventories Budget Monitoring Training and Guidance	12	4

Risk Area	Risk	Mitigation	Inherent Score	Residual Score
Procurement (Payments)	Redirection of payments to third party bank accounts through fraudulent submission of changes in bank details	Restrictions on officer abilities to modify supplier bank details Checking, review and authorisation procedures Training and Guidance	16	8
Payroll (Bogus employees)	Creation of bogus ('ghost') employees	Documentary evidential requirements Checking, review and authorisation procedures Independent headcount reconciliation	9	3
Payroll (Overtime/Claims)	Fraudulent overtime or expenses claims	Documentary evidential requirements Checking, review and authorisation procedures	9	4
Human Resources (Applications)	False employment applications	Documentary evidential requirements Checking, review and authorisation procedures	12	4
Human Resources (Sickness)	False claims for sickness absence	Documentary evidential requirements Checking, review and authorisation procedures	12	4
Planning	Intentionally false or misleading information contained within planning applications	Documentary evidential requirements Officer site visits Checking, review and authorisation procedures	12	4
Grant Aid	Fraudulent grant applications for work or activities not carried out or by ineligible groups or individuals	Documentary evidential requirements Knowledge of local community groups and individuals	9	3
Money Laundering	Money Laundering, often in the form of significant cash overpayments then followed by an electronic or cheque refund	Anti-Money Laundering Policy and Procedures Reporting channels to Money Laundering Reporting Officer (MLRO) and Internal Audit Reviews of customer account credit balances Limited cash transactions Training and Guidance	12	3

Risk Area	Risk	Mitigation	Inherent Score	Residual Score
Internal Fraud and Corruption (Inducements)	Inappropriate favourable treatment of a supplier/customer/ applicant by a Council officer, often in exchange for financial reward.	Code of Conduct Disciplinary Procedure Whistleblowing Procedure Declarations of Interest Review/authorisation processes for decision making Training and Guidance	**9**	**4**
Internal Fraud and Corruption (Theft)	Theft of cash or other physical assets	Limited petty cash floats Bank reconciliation Inventories Training and Guidance	**9**	**4**
Internal Fraud and Corruption (Payments)	Redirection of payments to personal bank accounts	Restrictions on officers modifying supplier bank details Checking, review and authorisation procedures Training and Guidance Detection and prevention of ‘phishing’ emails	**9**	**4**
Internal Fraud and Corruption (Improper Use)	Improper personal use of Council assets (such as vehicles and fuel)	Code of Conduct Tachographs Monitoring of fuel usage Vehicle Tracking (Masternaut) Training and Guidance	**9**	**4**
Licensing	Fraudulent applications for new or renewed licences	Documentary evidential requirements Checking, review and authorisation procedures Data-matching exercises through NFI	**12**	**4**

Risk Area	Risk	Mitigation	Inherent Score	Residual Score
Insurance Fraud (Claims)	False, inflated or duplicate claims	Documentary evidential requirements Checking, review and authorisation procedures Internal and external (insurance company) monitoring of claims	12	3
Cybercrime (System Outage)	System outage, operational disruption, financial loss and / or reputational damage as a result of a targeted cyber attack	Firewalls and similar ICT security systems Disaster Recovery and Business Continuity Plans Frequent initial and refresher training for all staff Immutable technology for data storage Annual Cyber Security penetration testing XDR monitoring for all Endpoints Endpoint protection technologies	25	15
Cybercrime (Data Breach)	Loss of data and / or data breach as a result of targeted cyber attack	Firewalls and similar ICT security systems Disaster Recovery and Business Continuity Plans Frequent initial and refresher training for all staff Immutable technology for data storage Annual Cyber Security penetration testing XDR monitoring for all Endpoints Endpoint protection technologies	25	15
Cybercrime (Internal Theft)	Intentional theft of data by an employee	Code of Conduct Disciplinary Procedure Frequent initial and refresher training for all staff	16	8