Leicestershire County Council - Fraud Risk Assessment 2024/25

Under the 'Identify risks' principle of the CIPFA Code of Practice on Counter Fraud (2014) there are recommendations that fraud risks are routinely considered as part of the organisation's risk management arrangements and that the organisation identifies the risks of bribery and corruption and the importance of behaving with integrity in its governance framework.

The Internal Audit Service (IAS) performs a biennial fraud risk assessment and uses the results to direct both general audit resources and counter fraud resources accordingly. In essence the Fraud Risk Assessment is a key tool that informs the Internal Audit annual planning process. The assessment is informed by national and regional reports such as the Fighting Fraud and Corruption Locally (FFCL) report[1] which informs on the most reported causes of fraud within local government, the CIFAS Fraudscape Report 2024[2], and known outcomes from the National Fraud Initiative. Not all areas highlighted in national fraud intelligence are applicable to upper tier authorities, such as housing tenancy, revenue and benefits, but nevertheless there are fraud risks highlighted that have relevance to us as a county council, including procurement, payroll (insider) fraud, grant fraud, social care fraud and blue badge scheme fraud.

The National Fraud Initiative, administered by the Cabinet Office, matches data provided by public and private sector bodies to prevent and detect fraud. Many of the causes of fraud identified by FFCL are covered by the data matching exercise. The report issued in December 2022[3] reported an increase in

- pension fraud - includes individuals obtaining pension payments relating to a deceased person;
- concessionary travel passes - potential misuse of concessionary travel passes belonging to someone who has died;
- trade creditors - traders who intentionally or unintentionally submitted duplicate invoices for payment

The CIFAS Fraudscape report, which informs on both common and emerging frauds faced by private and public organisations, reports a slight reduction in reported insider / employee fraud compared to the same period in 2023, but still reports that, "*Employee fraud remains a key threat to organisations, especially in light of continued remote working and reduced supervision, leaving companies more vulnerable to a range of fraudulent and dishonest behaviours*".

The following table identifies details of:

- the fraud risks affecting local authorities as identified in national reports (n.b, includes those fraud risks pertinent to upper tier county councils only);
- the controls in place to mitigate the risk of fraud occurring;
- the final column discusses other information of interest.

---

[1] https://www.cifas.org.uk/secure/contentPORT/uploads/documents/FFCL%20-%20Strategy%20for%20the%202020's.pdf

[2] CIFAS Fraudscape 2024 6-month update https://www.fraudscape.co.uk/

[3] https://assets.publishing.service.gov.uk/media/638a131d8fa8f569f6a9d252/2022-12-02_NFI_report_2022__12v3__-_JQ.pdf

FRAUD RISK AREA (RAG GRADING)	FRAUD RISK DESCRIPTION	CONTROLS IN PLACE	ADDITIONAL INFORMATION
Procurement 146	At tendering and contract award stage due to • bid rigging; • collusion; • cartels; • bid evaluation (insider fraud).	• Commissioning & Procurement Strategy; • Contract Procedure Rules including defined process for the recording of receipt and opening of bids; • Employee Code of Conduct; • Declaration of Personal Interests – updated to provide clarity in circumstances when declaration of close personal relationship is required; • Specific article published regarding conflict of interest in procurement / tendering procedure; • Gifts & Hospitality Register and annual reminder of necessity to report all offers; • Fraud Training directed specifically towards procurement. Data matching in the biennial National Fraud Initiative exercise includes: • Payroll to Creditors (linked by bank account or address); • Payroll to Companies House (employees who appear to be registered directors of companies that LCC has traded with, or employees address appears to have links to the company directors or the company)	
	Post-contract award stage due to • overcharging; • duplicate invoicing; • under delivery on contract terms.	• Contract Management • No order, no pay. • Segregation of duties between the receipt of goods and invoice approvals.	

		Data matching in the biennial National Fraud Initiative exercise includes: • possible duplicate payments that may have arisen as a result of poor controls or fraudulent activity by suppliers and/or staff.	
Adult Social Care	Deprivation / Non-Declaration of Capital (to minimise or eliminate a service user's contribution to the costs of care).	• Signed declaration of accuracy of information supplied; • Proof of income / statements required; • Access to DWP online system for benefit checks; • Random independent checks by Senior Case Officers; • Access to NAFN Data Intelligence.	The Cabinet Office is seeking to reinstate social care data matching within the biennial National Fraud Initiative exercise from 2024, subject to the completion of a Legislative Reform Order (LRO) to amend the Local Audit and Accountability Act (LAAA) 2014. This will see data matching of personal budgets or care home residents against (i) deceased persons records to identify where invalid payments continue, (ii) other authorities' data with a view to identifying fraudulent duplicate claimants, and (iii) Land Registry / HMRC records to identify property ownership or recent disposals of property.
	Misuse of direct payments / personal budgets	• Monthly reports and alerts provided by DP card supplier; • Use of ATMs blocked; • Representative to act where service user lacks mental capacity; • Annual review includes financial review.	
	Residential settings claiming for deceased or fictitious residents	• Payment only made where a CPLI is in place; • CPLI suspended upon notification of death preventing further payment.	
	Financial abuse of vulnerable service users	• Review of case should concern be raised about ability to pay contribution;	

 		• Review of bank statements to identify unusual activity; • Safeguarding policies and procedures; • Referral to Office of Public Guardian for investigation.	
Children Social Care	Misuse of direct payments / personal budgets	• Monthly reports and alerts provided by DP card supplier; • Annual review includes financial review	
	Financial abuse of vulnerable service users	• Review of bank statements to identify unusual activity	
Blue Badge / Concessionary Travel Pass / Residential Parking Permits	Blue badges / concessionary travel passes / parking permits may be used by those not entitled to use them	'Tell Us Once' reports used to identify badges / passes that require cancelling. Data matching in the biennial National Fraud Initiative exercise includes: • Current badge/permit holders to DWP deceased persons records	
Insurance Claims	Fraudulent Insurance Claims received	Various methods used to validate statements made on claims	
Insider Fraud / Employee Fraud	Manipulation of official processes e.g. Setting up of a Ghost Employee	• Employee Code of Conduct • Gifts & Hospitality Policy • Declaration of Personal Interests Policy • Anti-Fraud & Corruption Strategy • Anti-Bribery Policy • Anti-Money Laundering Policy • Whistleblowing Procedures • Information & Data Governance Policy • Mandatory Fraud Awareness e-learning module, introducing refresher course which will need to be completed every two years	A wide range of "counter fraud" audits are undertaken regularly to manage the risk of employee fraud. This includes, for example, travel and subsistence allowances and procurement cards.
	False claims - Inflated travel and subsistence claims or overtime claims		
	Attendance & Absence - falsely claiming sick pay while either not being ill or working on another job		
	Theft of equipment, stationery or data		
	Waste Crime – theft of items disposed by public		

	Misuse of official assets or undertaking personal business during working time	• GDPR UK and Information Security Digital Learning e-learning module • Guidance published on Insider Fraud • Managers are responsible for ensuring that there is a strong internal control environment within their service areas, for example, by making sure that proper authorisation and approval controls are in place, e.g. payroll documentation, or that certain duties are divided amongst the team to prevent the risk of fraud or accidental error. Data matching in the biennial National Fraud Initiative exercise includes: • Payroll to Payroll (to identify individuals who may be committing employment fraud by failing to work their contracted hours because they are employed elsewhere or are taking long-term sickness absence from one employer and working for another employer at the same time); • Payroll to Companies House (employees who are registered directors of companies that LCC has traded with or employee addresses with links to company directors or the company); • Payroll to Creditors (linked by bank account or address).	
	Abuse of position e.g. misuse of procurement cards / imprest accounts / theft of income / misuse of returned blue badges		
	Abuse of Position - Corruption / Bribery		
	Money Laundering		
Employment Application / Recruitment	• No right to work in the UK • false identity • false qualifications • false references • concealment of key information for example reasons for breaks in employment history	Guidance and checklists for recruitment manager to follow includes • confirming right to work in UK • obtaining reason for gaps in employment history • take-up of references • ID checking • Obtain proof of qualifications	

		• checking professional registers for identified practice concerns	
Cybercrime	• phishing • hacking • mandate fraud • CEO ('bogus boss') fraud • malware • ransomware • theft of data	• Knowledge transfer via email, Sharepoint, ICT portal advising employees of scams and action to be taken. • Fraud awareness e-learning and ad hoc comms. • ICT Policies and Procedures • ICT controls, e.g. virus protection, firewalls, back-ups. • Defined processes underwriting changes to creditor / employee bank accounts.	The risk of cyber crime is included on, and monitored through, the Corporate Risk Register.
Economic & 3rd Sector	Fraudulent claims for grant payments - e.g. Winter Support Grant, Household Support Fund, LCC Communities Fund, Shire Grant	• Controls at application stage, e.g. confirmation of validity of organisations, verification of bank statements, constitutions etc. • Defined eligibility criteria. • Post-payment reviews of spend, outcomes etc.	
Pension Fund	Continued payments to deceased pension fund members	• Monthly mortality screening facilitated though screening bureau • Six monthly mortality screening to DWP records facilitated through the National Fraud Initiative to identify overseas deaths Data matching in the biennial National Fraud Initiative includes: • Pension records to DWP Deceased Persons record	Although cases have been identified through the NFI data matching exercise these have not been linked to fraudulent activity.
Activity level-based funding / payments	Over inflation of activity data by providers to obtain increased funding / payments from the Council	All departments • Contract Management • KPI monitoring	