NOTICE OF MEETING

Meeting:	**AUDIT COMMITTEE**
Date and Time:	**FRIDAY, 27 MARCH 2026, AT 10.00 AM**
Place:	**COUNCIL CHAMBER - APPLETREE COURT, BEAULIEU ROAD, LYNDHURST, SO43 7PA**
Enquiries to:	**E-mail: lee.ellis@nfdc.gov.uk** **Lee Ellis Tel: 023 8028 5719**

PUBLIC INFORMATION:

This agenda can be viewed online (https://democracy.newforest.gov.uk). It can also be made available on audio tape, in Braille and large print.

Members of the public are welcome to attend this meeting. The seating capacity of our Council Chamber public gallery is limited under fire regulations to 22.

Members of the public can watch this meeting live, or the subsequent recording, on the Council's website. Live-streaming and recording of meetings is not a statutory requirement and whilst every endeavour will be made to broadcast our meetings, this cannot be guaranteed. Recordings remain available to view for a minimum of 12 months.

PUBLIC PARTICIPATION:

Members of the public may speak in accordance with the Council's public participation scheme:

(a) on items within the Audit Committee's terms of reference which are not on the public agenda; and/or

(b) on individual items on the public agenda, when the Chairman calls that item. Speeches may not exceed three minutes.

Anyone wishing to attend the meeting, or speak in accordance with the Council's public participation scheme, should contact the name and number shown above no later than 12.00 noon on Tuesday, 24 March 2026.

Kate Ryan
Chief Executive

Appletree Court, Lyndhurst, Hampshire. SO43 7PA
www.newforest.gov.uk

AGENDA

Apologies

1. MINUTES

To confirm the minutes of the meeting held on 13 February 2026 as a correct record.

2. DECLARATIONS OF INTEREST

To note any declarations of interest made by members in connection with an agenda item. The nature of the interest must also be specified.

Members are asked to discuss any possible interests with Democratic Services prior to the meeting.

3. PUBLIC PARTICIPATION

To receive any public participation in accordance with the Council's public participation scheme.

4. OPEN SPACES AND PLAYGROUND SAFETY CHECKS (Pages 3 - 10)

To receive the Open Spaces and Playground Safety Checks report.

5. INTERNAL AUDIT PROGRESS REPORT 2025-26 (FEBRUARY 26) (Pages 11 - 34)

To receive the Internal Audit Progress Report 2025/26 (February 26).

6. INTERNAL AUDIT CHARTER AND RISK BASED PLAN 2026-27 (Pages 35 - 72)

To receive the Internal Audit Charter and Risk Based Plan 2026-27.

7. REGULATION OF INVESTIGATORY POWERS ACT 2000 AND INVESTIGATORY POWERS ACT 2016 (Pages 73 - 134)

To receive the Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 Report.

8. AUDIT COMMITTEE WORK PLAN (Pages 135 - 138)

To consider the Audit Committee's Work Plan.

9. ANY OTHER ITEMS WHICH THE CHAIRMAN DECIDES ARE URGENT

To: **Councillors**

Alan Alvey (Chairman)
John Adams (Vice-Chairman)
Kate Crisell
Jacqui England
Alan O'Sullivan

Councillors

Caroline Rackham
Janet Richards
Malcolm Wade
Richard Young

Audit Committee – 27 March 2026

Open Spaces and Playground Safety Checks Update

Purpose	For Review
Classification	Public
Executive Summary	New Forest District Council is committed to providing an effective maintenance regime for its Playground and Play Equipment, in order to comply with statutory responsibilities and health and safety obligations. This paper outlines the agreed approach to resolution of remaining outstanding audit actions. This is largely achieved via the alignment of the management of playgrounds within NFDC open spaces areas, including the maintenance, inspection and asset repair of play areas, with the recently adopted Playground and Play Equipment Policy 2025. This will ensure that all play areas and equipment provided by New Forest District Council are safe, inclusive, well maintained, and supportive of children's development encouraging wider community engagement.
Recommendation(s)	**That the Audit Committee note the proposed approach to the management of NFDC Playgrounds by the Public Realm and Sustainability Service.**
Reasons for recommendation(s)	The proposed approach will support consistency of standards across all NFDC playgrounds, improving customer experience, standardising NFDC processes, clarifying corporate responsibilities and reducing risk liabilities, and enable overdue audit actions to be completed and the audit closed.
Ward(s)	All
Portfolio Holder(s)	Councillor Geoff Blunden – Portfolio Holder for Environment and Sustainability

Strategic Director(s)	Tracey Coleman - Strategic Director – Place, Operations and Sustainability
Officer Contact	Chris Noble Assistant Director for Place Operations 02380 285389 Chris.Noble@nfdc.gov.uk

Introduction and background

1. NFDC maintain a number of children's playgrounds across the New Forest District area – some managed by the NFDC Housing Landlord Service, others managed by the NFDC Public Realm and Sustainability Service.

2. In 2025, NFDC adopted the Playground and Play Equipment Policy, developed by the Housing Landlord Service. The purpose of this policy is to ensure that all play areas and equipment provided by New Forest District Council are safe, inclusive, well maintained, and supportive of children's development encouraging wider community engagement.

3. To support consistency of standards across all NFDC playgrounds, it is proposed that both services operate in accordance with the 2025 policy. This would improve customer experience, standardise NFDC processes, clarify corporate responsibilities and reduce risk liabilities of playground sites.

Playgrounds managed by the Grounds Maintenance Team

4. The following playgrounds are (or will be) managed (inspected, maintained and repaired) as Open Spaces assets by the Grounds Maintenance Team, within the Public Realm and Sustainability Service:

	Site	**Location**	**W3W**
1	Buckland Gardens Play	Lymington	impulsive.finishers.tight
2	Foxgloves Play	Bransgore	bespoke.once.slack
3	Greenwood Close Play	New Milton	onwards.green.eternally
4	Heatherstone Play	Sopley	slug.anchorman.bluffing
5	Heatherstone Trail	Sopley	hologram.spark.orbited
6	Nursery Close Play	Hordle	even.otherwise.pickles
7	Pinetops Close Play	Pennington	tech.sunblocks.nags
8	Torreyana Gardens Play	Pennington	birthdays.lingering.juggles
9	Lakeside Way North	Totton	headliner.disclose.stow

10	Woodway Road	Totton	fattening.inspector.chuckling
12	Lakeside Way South	Totton	luggage.alarm.overheat
	Sites due to be transferred to NFDC Spring 2026		
13	Fieldhouse Way	Lymington	dragons.sprayer.reactions
14	Knight Gardens	Lymington	clicker.robe.retain
15	Caspars Way	Fordingbridge	validated.forever.media
16	Chard Lane	Ringwood	shrub.craft.popped
17	Yarrow Lane	Ringwood	earphones.pastels.captive
18	Hopclover Way	Ringwood	wage.fetches.bookcases

Playground Audit

5. In 2023, an internal audit was carried out of NFDC Open Spaces Playgrounds. This audit recommended 12 Management Actions. 7 of these are now closed. Of the remaining actions, 2 are high priority and 3 are medium priority.

6. The adoption of the Playground and Play Equipment Policy by Housing Landlord Services in 2025 has provided an opportunity to address the audit actions by aligning to an adopted standard rather than creating a new policy just for the playgrounds in areas managed by the Public Realm and Sustainability team. The benefits of this approach include speed of implementation, avoidance of duplication of effort, and ensuing a consistent standard that doesn't conflict with the management procedures of other NFDC departments for similar assets. Support for this approach will enable overdue audit actions to be completed and the audit closed.

7. The two remaining high priority actions, along with details of how they are being closed, is shown in the table below.

Management Action	**Resolution**
1.1 Critically review assets and inspection timescales based on 'Risk and Likelihood' and formalise site and play equipment inspection schedule.	The Housing Landlord Policy sets standard schedules and procedures for undertaking routine visual, operational, main annual and bespoke inspections in housing playgrounds. These schedules and procedures have been adopted across open spaces playgrounds as standard.

1.2 Open Spaces to draft a Playgrounds and Play Equipment Policy covering the sites and equipment where compliance responsibility rests with Open Spaces. The policy will set out the purpose, legal requirements, responsibilities, methodology, arrangements, and process, set out a review period frequency and append a schedule of sites and equipment. The policy is to be presented to EMT and consulted through safety panels.	The Open Spaces approach will align to the Housing Landlord Services policy, to prevent duplication or diverging approaches within the organisation.

8. To determine the required frequency of the "Operational" check, required every 1-3 months, there will be the annual undertaking of a risk assessment which will then inform the Operational Inspection schedule for each playground (i.e. 1, 2 or 3 monthly)

9. There will also be the following key differences between the Housing Landlord Services policy, and the approach taken by the Public Realm and Sustainability Team, as follows:

    a. Service specific roles and responsibilities will be different for open spaces versus housing playgrounds

    b. Procedures for the reporting of repairs and logging asset inspections will be different between the open spaces and housing services e.g. contact phone numbers/email, due to established processes, embedded software and pre-existing contracts

10. The three remaining medium priority actions, along with details of how they are being closed, is shown in the table below.

Management Action	**Resolution**
2.1 The Assistant Director for Place and Operations to assign a lead Place and Operations Officer to undertake a fundamental review of the cross service arrangements where responsibility rests with Place and Operations. The review to consider compliance activities, roles, responsibilities, efficiencies, reporting and data collection, budgets, and compliance monitoring. The data gathered from the review will inform Observation 1, 1.2 and 1.2 Investigate Revisions	The alignment with the Housing Landlord Services policy will address immediate concerns regarding roles, responsibilities and monitoring.

options regarding current Asset Inspection Criterion and IT Systems to track actions.	
3.1 Introduce Annual Reviews of Open Space Play Parks and Play Equipment Risk Assessments	Further to paragraph 8 above, this will be undertaken to determine inspection frequency, and reviewed annually.
5.1 Place and Operations to review the governance arrangements for health and safety compliance activities to provide oversight and assurance.	Reporting mechanisms will be developed so that compliance can be monitored and reported on in a timely manner.

Corporate plan priorities

11. This proposal supports the following Corporate Plan Priorities:

    a. People Priority 2: Empowering our residents to live healthy, connected and fulfilling lives – by providing access to high quality, safe playgrounds which encourage physical activity and social integration.

    b. Place Priority 3: Caring for our facilities, neighbourhoods and open spaces in a modern and responsive way – by taking a consistent and proactive approach to the management of all NFDC playgrounds, prioritising the health and safety of facilities.

Options appraisal

12. The following options were considered in the development of this proposal:

    a. Create a new playground management policy specific to play areas in open spaces managed my NFDC Grounds Maintenance Team. This would likely conflict with the procedures and standards recently approved for housing playgrounds, creating mixed expectations for residents and visitors and potentially creating confusion over corporate liability.

    b. Align as closely as possible with the recently approved Playground and Play Equipment Policy to support consistency of standards across all NFDC playgrounds, improving customer experience, standardising NFDC processes, clarifying corporate responsibilities and reducing risk liabilities.

13. Option b. offers a wide range of benefits and reduces corporate risks for NFDC and is therefore the recommended approach.

Consultation undertaken

14. Colleagues across multiple NFDC services have been consulted in the development of this proposal, including those in Housing, Planning, Transformation and Audit. Subject to approval of the approach, further consultation will be carried out in the detailed implementation of this proposal.

Financial and resource implications

15. There are no direct financial or resource implications arising from this proposal. The approach put forward seeks to reduce duplication of effort, align corporate procedures and improve the quality and longevity of corporate assets.

Legal implications

16. The proposed approach seeks to reduce corporate liability and clarify legal responsibilities in relation to the management of NFDC playgrounds. Further consultation with Legal may be needed in the event that inspections schedules are varied following risk assessment.

Risk assessment

17. Risks associated with the approach are minimal but include the operational and legal risk of running slightly different processes between NFDC services (as outlined in paragraph 23).

Environmental / Climate and nature implications

18. Improving the inspection, maintenance and repair procedures of playgrounds in NFDC open spaces should improve asset condition, increasing equipment longevity and reducing material wastage/replacement.

Equalities implications

19. Standardising the NFDC approach to playground management across housing and open spaces sites will support access to high quality play areas across the district and encourage inclusion in physical activity, regardless of which service area manages the site. The recommended approach will bring consistency of safety and quality of play areas, regardless of geographical location.

Crime and disorder implications

20. Improving the condition and inspection schedule of playgrounds could have a positive impact on the look and feel of sites, encouraging increased footfall and helping to reduce antisocial behaviour.

Data protection / Information governance / ICT implications

21. No data protection/information governance or ICT implications arising from the recommendations due to no personal data being collected and no changes to existing software/hardware.

New Forest National Park / Cranborne Chase National Landscape implications

22. Improving the quality and safety of playgrounds in NFDC open spaces will positively impact the objectives of the New Forest National Park and Cranborne Chase National Landscape by encouraging recreation in specifically designed playgrounds rather than potentially in protected habitats. High quality playgrounds could increase visitor numbers, stay duration and economic activity, supporting communities and increasing appreciation for the local area.

Conclusion

23. The standardisation of management of playgrounds in NFDC open spaces supports consistency of standards across housing and open spaces play sites. The recommendations seek to reduce duplication of effort and reduce corporate risk, providing overall benefit for the residents and visitors of the New Forest District.

24. The Public Realm and Sustainability Service will work to embed the procedures outlined.

25. This will enable internal audit actions to be completed and closed.

Appendices:

None

Background Papers:

Playground and Play Equipment Policy 2025

This page is intentionally left blank

Audit Committee – 27 March 2026

Internal Audit Progress Report 2025-26 (February 26)

Purpose	For decision
Classification	Public
Executive Summary	In accordance with the Global Internal Audit Standards in UK Public Sector this report presents the Internal Audit Progress Report to 27th February 2026. The Internal Audit Progress Report, attached as Appendix A, provides the Audit Committee with an overview and key updates of internal audit activity and assurance work completed in accordance with the approved audit plan.
Recommendation(s)	**The Audit Committee are requested to note the Internal Audit Progress Report 2025-26 (February 2026) and approve the proposed changes to the audit plan.**
Reasons for recommendation(s)	To keep the Audit Committee appraised of internal audit activity and key updates relevant to the discharge of the Committee's role in relation to internal audit.
Ward(s)	All Wards
Portfolio Holder(s)	Councillor Jeremy Heron – Finance and Corporate
Strategic Director(s)	Alan Bethune, Strategic Director of Corporate Resources. S151 Officer
Officer Contact	Antony Harvey, Deputy Head of Southern Internal Audit Partnership 07784 265289 antony.harvey@hants.gov.uk

Introduction and background

1. The mandate for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015, which states:

   'A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.'

2. From 1 April 2025, the 'standards or guidance' in relation to internal audit are those laid down in the Global Internal Audit Standards (GIAS), Application Note: Global Internal Audit Standards in the UK Public Sector (Application Note) and the Code of Practice for the Governance of Internal Audit in UK Local Government. The collective requirements shall be referred to as the Global Internal Audit Standards in the UK Public Sector (the Standards).

3. The Southern Internal Audit Partnership have been externally assessed against conformance with the Global Internal Audit Standards in the UK Public Sector which concluded:

   'SIAP has achieved an excellent result of ***'generally achieves'*** *in this EQA in relation to the GIAS and Application Note. The IIA use the term 'general achievement' or 'general conformance' to indicate that "internal audit activities were performed in general conformance with the Global Standards."*

   Given SIAP's high level of performance and achievement with the GIAS, ***I do not make any formal recommendations in this report.***

   I am delighted to confirm that SIAP fully achieves 46 of the 52 Standards and generally achieves the remaining six Standards*. There are no partial conformances, or areas where the team do not conform with any Standards.'*

4. In accordance with proper internal audit practices (Global Internal Audit Standards in the UK Public Sector), the Chief Internal Auditor is required to provide a written status report to the Audit Committee, summarising:

   - ongoing confirmation or otherwise regarding independence, and impairments [Standard 7.1]
   - a summary of significant issues and escalation of matters of importance [Standard 8.1]

- overview and sufficiency of resourcing [Standards 8.2, 10.1, 10.2, and 10.3]
- communication of unresolved issues that fall outside of the Council's risk tolerance [Standard 11.5]
- update on progress and any changes to the annual audit plan [Standard 9.4]
- internal audit performance measures [Standard 12.2]
- status of 'live' internal audit reports and status on the implementation of management actions [Standard 15.2].

5. Appendix A summarises the activities of internal audit for the period to 27th February 2026. The progress report confirms that 56% of the agreed plan has reached the reporting stages (previously 34% as reported within the December 2025 update), with a further five review areas where fieldwork is complete and is currently under management review, with corresponding reports to follow in due course. There are two proposed plan deferments to 2026-27 for consideration and approval. All remaining reviews are in progress.

6. Two 2025-26 reports have been finalised since the previous progress update in December 2025. The audit of Transformation concluded with a Substantial Assurance Opinion however the audit of Engineering works concluded with a Limited Assurance Opinion and a summary is provided in section 10 of the report. Two further reports in relation to 2024-25 have also been finalised.

7. The report also provides an update on the Council's progress with implementing actions that have been agreed following audits, including confirmation that all actions have been completed in respect of two previous audit review areas. The number of overdue management actions remains low and is consistent with the position previously reported within the December 2025 progress update.

Corporate plan priorities

8. The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively. The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

Options appraisal

9. No alternative options have been considered as this report is a requirement under relevant legislation and standards.

Consultation undertaken

10. This report has been discussed with the Executive Management Team.

Financial and resource implications

11. The audit plan consists of 400 audit days including 18 audit days provided to the New Forest National Park Authority under the current Service Level Agreement. The Council's budget for 2025-26 reflects these arrangements.

Legal implications

12. The statutory requirement for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015. Internal audit functions within the UK Public Sector must conform with The Global Internal Audit Standards in the UK Public Sector (the Standards). The Standards require the Chief Internal Auditor to provide a written status report to the Audit Committee providing an overview and key updates of internal audit activity and assurance work completed in accordance with the approved audit plan. This report provides the Audit Committee with the progress report to 27th February 2026.

Risk assessment

13. The audit needs assessment follows a risk-based audit approach taking cognisance of the Council's risk register.

14. Failure to deliver an appropriate audit plan would increase the risk of failing within the Council's service delivery.

15. Failure to complete management actions or to act on the initial findings during the audit process will likely increase the chances of a negative outcome and/or delay required improvements to the Council's services.

Environmental / Climate and nature implications

16. There are no additional implications arising from this report.

Equalities implications

17. There are no additional implications arising from this report.

Crime and disorder implications

18. There are no additional implications arising from this report.

Data protection / Information governance / ICT implications

19. There are no additional implications arising from this report.

Appendices:	**Background Papers:**
Appendix 1 – Internal Audit Progress Report 2025-26 (February 26)	Internal Audit Plan 2025-26 Internal Audit Charter 2025-26 Internal Audit Progress Report 2025-26 (September 25) Internal Audit Progress Report 2025-26 (December 25)

This page is intentionally left blank

APPENDIX 1

Southern Internal Audit Partnership

Assurance through excellence and innovation

Internal Audit Progress Report

New Forest District Council – February 2026

Prepared by: Antony Harvey, Deputy Head of Partnership

1. Internal Audit Mandate

The mandate for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015, which states:

'5. (1) A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.

(2) Any officer or member of a relevant authority must, if required to do so for the purposes of the internal audit—

(a) make available such documents and records; and
(b) supply such information and explanations

as are considered necessary by those conducting the internal audit.'

The role of internal audit is best summarised through its definition within the Standards, as an:

'*An independent, objective assurance and advisory service designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes*.'

The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively.

The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

2. Internal Audit Standards

With effect from 1 April 2025, the 'Standards' against which internal audit within the public sector must conform are those laid down in the Global Internal Audit Standards, Application Note: Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government. The collective requirements are referred to as the Global Internal Audit Standards in the UK Public Sector.

3. Purpose of Report

In accordance with proper internal audit practices (Global Internal Audit Standards in the UK Public Sector), and the Internal Audit Charter the Chief Internal Auditor is required to provide a written status report to Senior Management and the Audit Committee, summarising:

- The monitoring of 'live' internal audit reports
- an update on progress against the annual audit plan and any subsequent revisions
- acknowledgement of any actual or perceived impairments to internal audit independence
- internal audit performance, planning and resourcing issues
- results of audit assignments and insights.

Internal audit reviews culminate in an opinion on the assurance that can be placed on the effectiveness of controls in place focusing on those designed to mitigate risks to the achievement of management objectives of the service area under review. Assurance opinions are categorised as follows:

Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

4. Resourcing

As Chief Internal Auditor I maintain responsibility for ensuring that there is a sufficient level of resource available, supported by an appropriate range of knowledge, skills, qualifications and experience to deliver the internal audit plan (2025-26) and in the fulfilment of the audit mandate and delivery of the internal audit strategy.

- **Human Resource -** the Southern Internal Audit Partnership has access to an appropriate range of knowledge, skills, qualifications and experience required to deliver the internal audit strategy and risk-based audit plan.
- **Financial Resource -** the Head of Southern Internal Audit Partnership will manage the internal audit budget to enable the successful implementation of the internal audit mandate and achievement of the plan. The budget includes the resources necessary for the function's operation, including training and relevant technologies and tools.
- **Technological Resource -** the internal audit function has the technology to support the internal audit process and regularly evaluates technological resources in pursuit of opportunities to improve effectiveness and efficiency.

5. Independence

As your chief internal auditor, I retain no roles or responsibilities that have the potential to impair my independence, either in fact or appearance. Internal auditors engaged in the delivery of the 2025-26 internal audit plan have had no direct operational responsibility or authority over any of the activities reviewed. I can confirm there has been no interference encountered relating to the scope, performance, or communication of internal audit work during the year to date in the delivery of the internal audit plan or the fulfilment of the internal audit mandate.

6. Impairments

There have been no impairments to internal audit activity during the year. The internal audit function has remained free from all conditions that threaten our ability to carry out responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. The internal audit team have maintained an unbiased mental attitude allowing them to perform engagements objectively enabling them to believe in their work product, with no compromise to quality, and no subordination to their judgment on audit matters, either in fact or appearance.

7. Rolling Work Programme

The internal audit plan for 2025-26 was originally presented to Senior Management and approved by the Audit Committee in March 2025. The audit plan remains fluid to provide a responsive service that reacts to the changing needs of the Council. Progress against the plan is detailed below.

Audit Review	Sponsor	Scoping Held	ToR Issued	Fieldwork Start	Draft Report	Final Report	Assurance Opinion	Comment
Town and Parish Councils – Shared Delivery Arrangements *	ADPO	02.09.24	07.10.24	11.11.24	12.05.25	23.01.26	**Limited**	* Included within 24-25 Annual Conclusion Report therefore excluded from 25-26 performance.
Environmental Enforcement - Clean Streets *	SDH&C	30.11.23	16.01.24	03.03.24	20.12.24		**Limited**	
Cemeteries *	ADPO	15.11.24	05.12.24	07.01.25	28.02.25	08.01.26	**Reasonable**	
Keyhaven – Income & PCard Expenditure *	SDH&C	10.12.24	20.01.25	20.01.25	24.04.25		**Reasonable**	
Corporate Plan and Performance Management	ADT	08.01.25	09.05.25	19.05.25	11.07.25	30.09.25	**Substantial**	
Transformation	ADT	30.07.25	16.10.25	10.11.25	22.12.25	26.01.26	**Substantial**	
Corporate Governance Framework – Complaints	SDCR	15.05.25	04.06.25	30.06.25	05.09.25	14.10.25	**Substantial**	
Asset Management – Corporate Estate	SDCR	27.01.26	20.02.26 (draft)					Fieldwork Mar-Apr.
Investment Property Management	SDCR	13.08.25	08.10.25	03.11.25	25.02.06			
Information Governance – SAR & DP2	SDCR	11.12.25	09.02.26					Fieldwork Mar-Apr.
Procurement	ADFIN	11.09.25	10.10.25	22.10.25	25.02.26			
Business Continuity	SDH&C	06.10.25	25.11.25	25.11.25				Fieldwork complete. Under management review. Close to be arranged.
Emergency Planning	SDH&C	06.10.25	19.11.25	24.11.25				Fieldwork complete. Under management review. Close to be arranged.

Audit Review	Sponsor	Scoping Held	ToR Issued	Fieldwork Start	Draft Report	Final Report	Assurance Opinion	Comment
Risk Management	ADT	15.01.26	16.02.26					Fieldwork Mar-Apr.
HR – Workforce Strategy and Wellbeing	ADT	16.10.25	11.12.25	10.02.26				
Safeguarding	SDH&C	22.09.25	30.10.25	06.11.25	19.01.26			
Treasury Management	ADFIN	12.12.24	27.01.25	12.05.25	10.09.25	02.10.25	**Substantial**	
Council Tax	SDCR	16.07.25	30.07.25	12.08.25	30.09.25	21.10.25	**Reasonable**	
Accounts Receivable & Debt Management	ADFIN	26.01.26	26.02.26					Fieldwork Mar-Apr.
Main Accounting and Reconciliations	ADFIN	16.09.25	12.11.25	27.11.25				Fieldwork complete. Under management review. Close to be arranged.
IT – Firewall Management and Monitoring	ADT	23.01.25	24.02.25	13.11.25				Fieldwork complete. Under management review. Close booked 23.03.26
Cyber Security Training and Awareness	ADT	13.05.25	23.06.25	14.07.25	22.09.25	16.10.25	**Reasonable**	
IT Disaster Recovery and Service Continuity	ADT	06.10.25	22.10.25	12.12.25				Fieldwork complete. Under management review. Close booked 25.03.26
Licencing (Temporary Event Notices, Premises and Personal Licenses)	SDH&C	06.02.25	03.04.25	12.05.25	30.07.25	26.08.25	**Substantial**	
Planning/Development Management	SDPOS	31.07.25	29.09.25	23.10.25	16.12.25			
Engineering works	ADPO	23.06.25	05.08.25	04.09.25	13.10.25	20.01.26	**Limited**	
Taxi Vehicle Licencing	SDH&C	14.01.26	20.02.26 (draft)					Fieldwork Mar-Apr.
Tenant Engagement	ADH	14.05.25	14.07.25	02.09.25	15.10.25	29.10.25	**Reasonable**	
Housing Asset Management – Analogue to Digital Switchover	ADH	22.10.25	25.11.25	05.12.25	10.02.26			
Housing Asset Management – Fire Safety	ADH	08.08.25	26.09.25	05.12.25				

Audit Review	Sponsor	Scoping Held	ToR Issued	Fieldwork Start	Draft Report	Final Report	Assurance Opinion	Comment
Waste Rollout – Phase Three (Bin order and delivery)	SDCR	10.12.25	19.12.25	05.01.26	26.02.26			

Audit Sponsor		Audit Sponsor	
Chief Executive	CX	Strategic Director Place, Operations & Sustainability	SDPOS
Chief Operating Officer / Deputy Chief Executive	COO	Assistant Director Place Operations	ADPO
Assistant Director Transformation	ADT	Assistant Director Place Development	ADPD
Assistant Director Strategy and Engagement (Monitoring Officer)	ADS&E	Strategic Director Housing & Communities	SDH&C
Strategic Director Corporate Resources (S151)	SDCR	Assistant Director Housing & Communities	ADH&C
Assistant Director Finance	ADFIN		

8. Adjustments to the Internal Audit Plan 2025-26

Internal Audit focus continues to be proportionate and appropriately aligned. The plan remains fluid and subject to on-going review and amendment, in consultation with the relevant audit sponsors, Senior Management, and the Audit Committee, to ensure internal audit are able to react to new and emerging risks and the changing needs of the Council.

Such amendments to the 2025-26 internal audit plan are detailed below with explanations for the proposed amendments.

Additions	**Audit Review**	**Reason for inclusion in the plan**
	Waste Rollout – Phase Three (Bin order and delivery) *	Direct request from the Council to assess the processes and controls for bin ordering and delivery for phase three of the new waste collection service.
Withdrawals	**Audit Review**	**Reason for removal from the plan**
	Open spaces *	Defer the audit due to on-going activity within the service to implement actions arising from previous audit reviews / to progress identified developments.
	Application Product Management	It is proposed to defer both ICT reviews to 2026-27 given there will be 3 ICT audits completed in 2025-26. Both NFDC ICT and SIAP have identified that there is not the capacity to facilitate a further two ICT audits within the remaining time available in 2025-26.
	Vulnerability Management	

* NB previously reported and agreed

9. Acceptance of Risk

Internal audit reporting protocols are in place to ensure that the scope of work and findings for all assignments are reported appropriately and that agreed management actions are approved by senior management.

Every effort will be made to resolve disagreements that may arise during the audit process. However, if, unresolved issues are considered by internal audit to fall outside of the Council's risk tolerance, these will be escalated to Senior Management and the Audit Committee as deemed necessary. There are no such instances to report from our delivery of the 2025–26 internal audit plan to date.

10. Executive Summaries of reports published concluding a 'Limited' or 'No' assurance opinion

Engineering Works		
Audit Sponsor	**Assurance opinion**	**Management Actions**
Assistant Director Place Operations	Limited	3 High, 6 Medium, 3 Low

Summary of key observations:

The 2022-23 Internal Audit review of Engineering Works concluded with a Limited Assurance opinion, identifying weaknesses in governance, operational processes and record-keeping across the service. While emergency works had been generally completed within required timescales and communication between supervisors and operatives was effective, there was reliance on a manual Job Log that did not support prioritisation or performance monitoring of the team. The audit also found an absence of documented procedures, lack of formalised roles and responsibilities, an unstructured paper-based filing system, and minimal forward planning from client services.

To assess the progress made in addressing the issues identified, a full internal audit review of the Engineering Works function was completed as part of the 2025-26 Internal Audit Plan. The purpose of the review was to assess the adequacy and effectiveness of arrangements in place for planning, prioritising, and managing engineering works, including both planned and reactive maintenance activities. This audit also concluded with a Limited Assurance opinion, reflecting on-going weaknesses across several aspects of governance, risk management, and operational control that require management attention.

The review found that while a new centralised system had been introduced to log and manage work requests, its reporting and data-analysis capabilities are not yet fully embedded. Testing of 30 work requests identified delays in completing jobs, with half of the sample not delivered within required timescales and several significantly overdue. Missing or incomplete data fields further reduced the reliability of records, and at the time of the audit, several jobs remained outstanding. The system's inability to generate performance-based reports was identified as a key barrier to effective oversight, limiting management's ability to monitor workload, track progress, or drive improvements through data-driven analysis. Subsequent to the audit, confirmation has been received that the rollout of Power BI reporting functionality, has been implemented to strengthen the information available with further refinement and enhancement expected to follow.

The audit also identified weaknesses in the documentation of operational processes. Evidence of site inspections was not consistently recorded, despite inspections being required before jobs are closed on the system, creating risks to quality assurance and service standards. In relation to risk

assessments, while all sampled works had an assessment in place, a number were only partially completed, lacking essential information such as attendance dates or operative names.

Management has agreed a number of actions to address these issues, with clear responsibilities and target dates set. Successful implementation is expected to improve performance monitoring, strengthen safety and quality assurance, and enhance operational resilience.

11. Analysis of 'Live Audit Reviews'

Audit Review	Report Date	Audit Sponsor	Assurance Opinion	Management Actions											
				Agreed			Pending			Complete			Overdue		
				L	M	H	L	M	H	L	M	H	L	M	H
Fleet Management (follow-up phase 2)	22.05.23	ADPO	Reasonable	2	3	4	-	-	-	2	2	4	-	1	-
Open Spaces and Playground Safety Checks	07.12.23	ADPO	Limited	3	7	2	-	-	-	3	4	-	-	3	2
Accounts Payable	13.06.25	ADFIN	Reasonable	2	3	-	-	-	-	2	2	-	-	1	-
Health and Safety	15.11.24	ADT	Reasonable	-	2	4	-	1	-	-	-	3	-	1	1
Information Governance – Data Retention/Records Management	16.04.25	SDCR	Reasonable	6	-	-	2	-	-	3	-	-	1	-	-
Housing Asset Management – Gas Safety	21.08.25	ADH	Reasonable	-	2	5	-	-	1	-	2	4	-	-	-
ICT Project Delivery	04.09.25	ADT	Limited	1	9	3	-	5	-	1	4	3	-	-	-
Corporate Plan and Performance Management	30.09.25	ADT	Substantial	5	4	4	-	-	-	5	3	4	-	1	-
Council Tax	21.10.25	SDCR	Reasonable	4	2	-	1	-	-	3	1	-	-	1	-
Cemeteries	08.01.26	ADPO	Reasonable	2	5	-	2	5	-	-	-	-	-	-	-
Engineering works	20.01.26	ADPO	Limited	3	6	3	2	4	1	1	2	2	-	-	-
Town and Parish Councils – Shared Delivery Arrangements	23.01.26	ADPO	Limited	1	9	1	1	9	1	-	-	-	-	-	-
Total				**29**	**52**	**26**	**8**	**24**	**3**	**20**	**20**	**20**	**1**	**8**	**3**

The management team have provided confirmation that all actions have been completed in respect of two previous audit review areas and are therefore not included within the table above. The respective review areas and report dates are:- Cyber Security Training and Awareness (Oct 2025) and Transformation (Jan 26).

Annexe 1

Overdue 'High Priority' Management Action

Open Spaces – Playground Safety Checks
Observation: Guidance, policies and operational procedures There are no current detailed procedure notes or guidance outlining the process and requirements within the Open Spaces Team, for example the criteria and timescales/frequency for maintenance checks. The Public Open Spaces Inspection Criteria Flowchart, which was last updated in Dec 2018, provides details of open spaces equipment to be checked and timescales however it does not appear that the flowchart has been revisited since its inception and there may be scope to reduce visits/inspection to certain sites based on guidance/legislation.
Risk: Hazards will not be identified and eliminated, which could lead to accidents and injuries.

Management Action	Original Due Date	Revised Due Date	Latest Service Update
1.1 Critically review assets and inspection timescales based on 'Risk and Likelihood' and formalise site and play equipment inspection schedule. (to be appended to policy, as set out in Action 1.2)	31.03.24	30.10.25 04.02.26 (Requested)	Internal Audit note that a new Playground and Play Equipment Policy (Housing Landlord Services), was presented to EMT on 24th February 2026, which will also apply to the play areas maintained by Open Spaces (pending confirmation).
1.2 Open Spaces to draft a Playgrounds and Play Equipment Policy covering the sites and equipment where compliance responsibility rests with Open Spaces. The policy will set out the purpose, legal requirements, responsibilities, methodology, arrangements, and process, set out a review period frequency and append a schedule of sites and equipment. The policy is to be presented to EMT and consulted through safety panels.	31.03.24	30.10.25 04.02.26 (Requested)	As above. NB There are also three medium priority overdue actions in relation to this audit which should be partially or fully addressed (pending confirmation).

Health & Safety
Observation: Contractor Health and Safety The Health and Safety policy states that The Council's corporate Control of Contractors Policy identifies the key services who undertake construction and maintenance projects. The corporate policy requires these services to complete their own specific arrangements for the management of construction projects and the control of contractors. These arrangements must include roles and responsibilities, procedures, training requirements, procurement requirements and template documents. Testing confirmed that a Control of Contractors policy is in place which includes detail on Health and Safety requirements for contractors, however this was last updated in 2021. The policy requires relevant areas of the Council to produce Standard Operating Procedures (SOPs) to enable compliance with regulations in this area. Testing found that the Operations Service had not yet produced a SOP as required.
Risk: Contractor Health and Safety may not be being addressed appropriately.

Management Action	Original Due Date	Revised Due Date	Latest Service Update
2.1 Review the 2021 Corporate Control of Contractors Policy and communicate throughout the organisation (High priority).	n/a	n/a	This high priority action was completed at the time of the audit.
2.2 Ensure all control of contractors standard operating procedures are reviewed and submitted to the Control of Contractors Working Group for approve. Once approved communicate to all relevant employees (High priority).	01.04.25	31.03.26	February 2026 update re the high and medium priority actions: Standard Operating Procedures (SOPs) for Corporate Resources & Transformation and Estates & Valuations have been implemented, are held on SharePoint and training has been provided to all relevant employees. SOPs for Housing and Communities were agreed in January. Formal cascade to staff & associated training is outstanding. SOPs for Place, Operations and Sustainability have been drafted and consultation has been undertaken with relevant services. Additional

			detail is required in relation to working with other services in the Council such as Housing. The SOPs will need to be considered and approved by the control of contractors working group. Due to staff changes and workload pressures, progressing the actions has been delayed. The provision of training is dependent upon completion of 2.2.

Annexe 2

Overdue 'Low & Medium Priority' Management Actions

Audit Review	Report Date	Opinion	Priority		Due Date	Revised Due Date
			Low	Medium		
Fleet Management (follow-up phase 2)	22.05.23	**Reasonable**		**1**	31.03.24	30.11.25 30.01.26 Requested
Open Spaces and Playground Safety Checks	07.12.23	**Limited**		**1**	31.03.24	30.10.25 04.02.26 Requested
				2	31.05.24	30.10.25 04.02.26 Requested
Accounts Payable	13.06.24	**Reasonable**		**1**	31.03.25	31.03.26
Health and Safety	15.11.24	**Reasonable**		**1**	01.08.25	31.03.26
Information Governance – Data Retention/Records Management	16.04.25	**Reasonable**	**1**		31.01.26	31.05.26
Corporate Plan and Performance Management	30.09.25	**Substantial**		**1**	30.11.25	Requested
Council Tax	21.10.25	**Reasonable**		**1**	30.11.25	30.06.26
Total			**1**	**8**		

Annexe 3

Southern Internal Audit Partnership - Performance Measures

Performance Measure	Regularity	Target	Actual 25-26	Status	Direction of Travel
1. Percentage of the agreed audit plan completed (issue of draft / final report)	Ongoing	90%	56%		
2. Audits delivered within agreed timescales (% year to date)					
○ To issue of draft report	Ongoing	80%	20%		
○ To issue of final report	Ongoing	80%	33%		
3. Conformance with the Global Internal Audit Standards in the UK Public Sector	Annual	Generally conforms	Generally conforms		
4. Audits conducted optimising the effective use of data analytics (% year to date)	Ongoing	60%	53%		
5. Stakeholder satisfaction (annual survey)					
○ Audit Committee	Annual	90%	100%		
○ Senior Management		90%	94%		
○ Key Contacts		90%	99%		
6. Internal audit effectively communicates with key stakeholders					
○ Audit Committee	Annual	90%	100%		n/a
○ Senior Management		90%	100%		n/a
○ Key Contacts		90%	99%		n/a
7. Sufficiency of input to and discussion of the internal audit plan					
○ Audit Committee	Annual	90%	100%		n/a
○ Senior Management		90%	100%		n/a
8. Appropriate focus on key risks					
○ Audit Committee	Annual	90%	100%		n/a
○ Senior Management		90%	100%		n/a
○ Key Contacts		90%	100%		n/a

33

This page is intentionally left blank

Audit Committee – 27 March 2026

Internal Audit Charter and Risk Based Plan 2026-27

Purpose	For decision
Classification	Public
Executive Summary	In accordance with Regulations and Standards: • the Council must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance. • all internal audit providers are required to implement and maintain an 'Internal Audit Charter'. • internal audit must create a risk-based internal audit plan that supports the achievement of the organisation's objectives. The internal audit charter is defined as 'a formal document that includes the internal audit function's mandate, organisational position, reporting relationships, scope of work, types of service, and other specifications' and is reported to the Audit Committee annually. The risk based internal audit plan for 2026-27 has been developed at a strategic level providing a value adding, and proportionate level of assurance aligned to the Council's Corporate Plan Priorities. The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

Recommendation(s)	**The Audit Committee are invited to review and approve the Internal Audit:** **Charter 2026-27 (Appendix 1); and** **Risk-Based Plan 2026-27 (Appendix 2).**
Reasons for recommendation(s)	In line with the Standards, the Audit Committee are responsible for the governance of the Council and it is imperative they are therefore engaged in the review and approval of the internal audit mandate and charter; and risk based internal audit plan.
Ward(s)	All Wards
Portfolio Holder(s)	Councillor Jeremy Heron – Finance and Corporate
Strategic Director(s)	Alan Bethune, Strategic Director of Corporate Resources. S151 Officer
Officer Contact	Antony Harvey Deputy Head of Southern Internal Audit Partnership 07784 265289 antony.harvey@hants.gov.uk

Introduction and background

1. The mandate for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015, which states:

   'A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.'

2. From 1 April 2025, the 'standards or guidance' in relation to internal audit are those laid down in the Global Internal Audit Standards (GIAS), Application Note: Global Internal Audit Standards in the UK Public Sector (Application Note) and the Code of Practice for the Governance of Internal Audit in UK Local Government. The collective requirements shall be referred to as the Global Internal Audit Standards in the UK Public Sector (the Standards).

3. The Southern Internal Audit Partnership have been externally assessed against conformance with the Global Internal Audit Standards in the UK Public Sector which concluded:

'SIAP has achieved an excellent result of ***'generally achieves'*** *in this EQA in relation to the GIAS and Application Note. The IIA use the term 'general achievement' or 'general conformance' to indicate that "internal audit activities were performed in general conformance with the Global Standards."*

Given SIAP's high level of performance and achievement with the GIAS, ***I do not make any formal recommendations in this report.***

I am delighted to confirm that SIAP fully achieves 46 of the 52 Standards and generally achieves the remaining six Standards. *There are no partial conformances, or areas where the team do not conform with any Standards.'*

4. The Standards (6.2) require all internal audit providers to implement and maintain an 'Internal Audit Charter'. The internal audit charter is defined as 'a formal document that includes the internal audit function's mandate, organisational position, reporting relationships, scope of work, types of service, and other specifications'

5. Standard 11.3 (Communicating Results) references the possibility that a chief internal audit may be required to make a conclusion at the level of the organisation about the effectiveness of governance, risk management and/or control. Section 10B of the Application Note makes it a mandatory requirement in the UK public sector, for the chief internal auditor to prepare such an overall conclusion at least annually in support of wider governance reporting. This overall conclusion must encompass governance, risk management and control. The requirement for an overall conclusion must also inform planning carried out under GIAS Standard 9.4 (Internal Audit Plan).

6. In accordance with the Standards (9.4) there is a requirement that internal audit must create a risk-based internal audit plan that supports the achievement of the organisation's objectives. The internal audit plan provides the mechanism through which the Chief Internal Auditor can ensure most appropriate use of internal audit resources to fulfil the audit mandate and delivery of the internal audit strategy.

7. The aim of internal audit's work programme is to provide independent and objective assurance to management, in relation to the business activities; systems or processes under review that:

- The framework of internal control, risk management and governance is appropriate and operating effectively; and
- Risks to the achievement of the Council's objectives are identified, assessed and managed to a defined acceptable level.

Internal Audit Charter 2026-27

8. The internal audit charter is reported to the Audit Committee annually for review and approval. Bar updates to reflect the change of job title for the Strategic Director of Corporate Resources, there have been no further revisions to the Internal Audit Charter since it was last approved by the Audit Committee in October 2025. A copy is attached as Appendix 1.

Internal Audit Risk-Based Plan 2026-27

9. The proposed risk based internal audit plan for 2026-27 is attached at Appendix 2 and has been developed at a strategic level providing a value adding, and proportionate level of assurance aligned to the Council's Corporate Plan Priorities. It is based on a range of inputs including review of the Council's Principal Risk Register and Service Risk Registers, sector knowledge and discussions with Directorate Management Teams.

10. Internal audit focus should be proportionate and appropriately aligned, and as such, only high and medium priority reviews identified during the planning process are incorporated within the Internal Audit Plan. The exception to this is where 'mandatory' audits (for example to certify the accuracy of grant claims to meet funding requirements) or specific management requests have been raised and sufficient capacity is available.

11. The audit plan will remain fluid to ensure internal audit's ability to react to the changing needs of the Council. Any additions to the plan must be able to clearly demonstrate a contribution to the audit conclusion on risk management, control and governance.

12. Any changes to the plan (including advisory assignments) will be transparently reported to the Executive Management Team and the Audit Committee during the course of the year for approval as part of our regular Progress Reports.

13. The Internal Audit Charter ensures the Chief Internal Auditor has sufficient resource necessary to fulfil the requirements and expectations to deliver an internal audit conclusion.

14. Significant matters that jeopardise the delivery of the plan, or require changes to the plan will be identified, addressed and reported to the Audit Committee, through regular progress reports.

15. The endorsement and sponsorship of the plan(s) at Member / Executive officer level will assist in providing the engagement and buy-in of staff at an operational level to ensure the outcome of audit reviews are optimised.

Corporate plan priorities

16. The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively. The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

Options appraisal

17. No alternative options have been considered as this report is a requirement under relevant legislation and standards.

Consultation undertaken

18. This report has been discussed and agreed with the Executive Management Team.

Financial and resource implications

19. The audit plan will consist of 370 audit days including 18 audit days provided to the New Forest National Park Authority under the current Service Level Agreement. The Council's budget for 2026-27 reflects these arrangements.

Legal implications

20. The statutory requirement for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015. Internal audit functions within the UK Public Sector must conform with The Global Internal Audit Standards in the UK Public Sector (the Standards). The Standards require all internal audit providers to implement and maintain an internal audit charter; and create a

risk-based internal audit plan that supports the achievement of the organisation's objectives.

Risk assessment

21. The audit needs assessment follows a risk-based audit approach taking cognisance of the Council's risk registers. Failure to deliver an appropriate audit plan would increase the risk of failing within the Council's service delivery.

Environmental / Climate and nature implications

22. There are no additional implications arising from this report.

Equalities implications

23. There are no additional implications arising from this report.

Crime and disorder implications

24. There are no additional implications arising from this report.

Data protection / Information governance / ICT implications

25. There are no additional implications arising from this report.

Appendices:	**Background Papers:**
Appendix 1 – Internal Audit Charter 2026-27 Appendix 2 – Risk Based Internal Audit Plan 2026-27	None

APPENDIX 1

Southern Internal Audit Partnership

Assurance through excellence and innovation

NEW FOREST DISTRICT COUNCIL

Internal Audit Charter
2026-27

Prepared By: Antony Harvey, Deputy Head of Southern Internal Audit Partnership

March 2026

1. Introduction

The Global Internal Audit Standards, issued by the Institute of Internal Auditors and effective in the UK Public Sector from April 2025, guide the worldwide professional practice of internal auditing and serve as a basis for evaluating and elevating the quality of the internal audit function.

While the Global Internal Audit Standards apply to all internal audit functions, it is acknowledged that internal auditors in the public sector work in a political environment under governance, organisational and funding structures that differ from those of the private sector.

Consequently, internal audit practitioners working in, or for, the UK public sector are required to apply the Global Internal Audit Standards subject to the interpretations and requirements of the Application Note: Global Internal Audit Standards in the UK public sector, issued by Relevant Internal Audit Standard Setters (RIASS).

In addition, relevant public sector bodies are also required to apply the Chartered Institute of Public Finance & Accountancy (CIPFA) Code of Practice for the Governance of Internal Audit in UK Local Government which provides a conduit for meeting the essential conditions for governance set out in the Global Internal Audit Standards, tailored for UK local government.

The collective requirements shall be referred to as the Global Internal Audit Standards in the UK Public Sector.

The Standards require all internal audit providers to implement and maintain an 'Internal Audit Charter'.

The internal audit charter is defined as *'a formal document that includes the internal audit function's mandate, organisational position, reporting relationships, scope of work, types of service, and other specifications'*

2. Definitions

The Global Internal Audit Standards in the UK Public Sector apply the following definitions:

The Board – *'the governing body authorised to provide the internal audit function with the appropriate authority, role, and responsibilities.'* At New Forest District Council ('the Council') this shall mean the Audit Committee.

Senior Management – *'the highest level of executive management of an organisation that is ultimately accountable to the Board for executing the organisation's strategic decisions, typically a group of persons that includes the Chief Executive Officer or Head of Organisation'*. At the Council this shall mean the Executive Management Team (EMT).

3. Internal Audit Mandate

The mandate for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015, which states:

> *'5. (1) A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.*
>
> *(2) Any officer or member of a relevant authority must, if required to do so for the purposes of the internal audit—*
>
> *(a) make available such documents and records; and*
> *(b) supply such information and explanations*
>
> *as are considered necessary by those conducting the internal audit.*
>
> *(3) In this regulation "documents and records" includes information recorded in an electronic form.'*

From 1 April 2025, the *'standards or guidance'* in relation to internal audit are those laid down in the Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government.

The scope of internal audit includes both assurance and advisory services covering the entire breath of the Council, including all activities, assets, and personnel of the organisation.

Fraud investigations may also be commissioned which will be conducted by the Southern Internal Audit Partnership's Counter Fraud Unit.

4. Authority, Roles and Responsibilities

Authority

The Chief Internal Auditor is positioned at a level in the organisation that enables internal audit services and responsibilities to be performed independently of management and with objectivity, enabling escalation as appropriate.

The Chief Internal Auditor reports functionally to the Audit Committee, and organisationally to the Strategic Director of Corporate Resources (Section 151 Officer), who is a member of the Executive Management Team and has statutory responsibility as proper officer under Section 151 of the Local Government Act 1972, for ensuring an effective system of internal financial control and proper financial administration of the Council's affairs.

The Chief Internal Auditor has direct access to the Chief Executive who carries the responsibility for the proper management of the Council and for ensuring that the principles of good governance are reflected in sound management arrangements.

The Chief Internal Auditor has direct access to the Council's Monitoring Officer where matters arise relating to Chief Executive responsibility, legality and standards.

Where it is considered necessary to the proper discharge of the internal audit function, the Chief Internal Auditor has direct access to elected Members of the Council and in particular those who serve on committees charged with governance (i.e. the Audit Committee). Private meetings, without senior management present, are also be offered to the Chair of the Audit Committee.

Should organisation structures change, senior management and the Audit Committee will ensure that the reporting line of the Chief Internal Auditor remains with a member of the Executive Management Team and retains the relevant access to Members and officers as outlined above.

It is recognised that the Chief Internal Auditor supervises assurance services related to activities that are managed by the Strategic Director of Corporate Resources to whom the Chief Internal Auditor reports administratively, however, this perceived impairment is mitigated through overview from the Head of Southern Internal Audit Partnership, and the alternative reporting lines detailed above.

Internal audit reporting protocols are in place to ensure that the scope of work and findings for all assignments are reported appropriately and that agreed management actions are approved by senior management.

Every effort will be made to resolve disagreements that may arise during the audit process. However, if, unresolved issues (such as limitations to the scope of work or failure to agree appropriate actions in response to audit findings) are considered by internal audit to fall outside of the Council's risk tolerance, these will be escalated to the relevant Assistant Director and Strategic Director in the first instance and then to the Strategic Director of Corporate Resources, Chief Executive and Audit Committee as deemed necessary.

The Executive Management Team and the Audit Committee authorises the internal audit function to:

- Have full and unrestricted access to all functions, data, records, information, physical property, and personnel pertinent to carrying out internal audit responsibilities. Internal auditors are accountable for confidentiality and safeguarding records and information. Such access shall be granted on demand and not subject to prior notice.
- Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques, and issue communications to accomplish the function's objectives.
- Obtain assistance from the necessary personnel of the Council and other specialised services from within or outside the Council to complete internal audit services.

Role

The role of internal audit is best summarised through its definition within the Global Internal Audit Standards in the UK Public Sector, as:

'An independent, objective assurance and advisory service designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.'

Purpose

Internal audit strengthens the Council's ability to create, protect, and sustain value by providing the Audit Committee and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

Internal audit enhances the Council's:

- Successful achievement of its objectives.
- Governance, risk management, and control processes.
- Decision-making and oversight.
- Reputation and credibility with its stakeholders.
- Ability to serve the public interest.

Internal audit is most effective when:

- It is performed by competent professionals in conformance with the Global Internal Audit Standards in the UK Public Sector, which are set in the public interest.
- The internal audit function is independently positioned with direct accountability to the board.
- Internal auditors are free from undue influence and committed to making objective assessments

The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively. The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

Responsibility

The responsibility for maintaining an adequate and effective system of internal audit within the Council lies with the Strategic Director of Corporate Resources, as the authority's Chief Finance Officer (S151 Officer).

For the Council, internal audit is provided by the Southern Internal Audit Partnership. The Chief Internal Auditor, Antony Harvey (Deputy Head of Southern Internal Audit Partnership), is responsible for effectively managing the internal audit activity in accordance with the Global Internal Audit Standards in the UK Public Sector.

The Chief Internal Auditor

Has the responsibility to:

- At least annually, develop a risk-based internal audit plan engaging with the Audit Committee and Executive Management Team and submit the plan to the Audit Committee for review and approval.
- Communicate the impact of resource limitations on the internal audit plan to the Audit Committee and Executive Management Team.
- Review and adjust the internal audit plan, as necessary, in response to changes in the Council's business, risks, operations, programs, systems, and controls.
- Communicate with the Audit Committee and Executive Management Team if there are significant interim changes to the internal audit plan.

- Ensure internal audit engagements are performed, documented, and communicated in accordance with the Global Internal Audit Standards in the UK Public Sector (and relevant laws and/or regulations).
- Follow up on engagement findings and confirm the implementation of management actions or action plans and communicate the results of internal audit services to the Audit Committee and Executive Management Team periodically and for each engagement as appropriate.
- Ensure the internal audit function collectively possesses or obtains the knowledge, skills, and other competencies and qualifications needed to meet the requirements of the Global Internal Audit Standards in the UK Public Sector and fulfil the internal audit mandate.
- Identify and consider trends and emerging issues that could impact the Council and communicate to the Audit Committee and Executive Management Team as appropriate.
- Consider emerging trends and successful practices in internal auditing.
- Establish and ensure adherence to methodologies designed to guide the internal audit function.
- Ensure awareness of the Council's relevant policies and procedures, however should such policies and procedures conflict with the internal audit charter or the Global Internal Audit Standards in the UK Public Sector, such conflicts will be resolved or documented and communicated to the Audit Committee and Executive Management Team.
- Coordinate activities and consider relying upon the work of other internal and external providers of assurance and advisory services.
- Deliver an annual conclusion that can be used by the Council to inform its annual governance statement. The annual conclusion will conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control. Discuss the annual conclusion with the Audit Committee and Executive Management Team and submit the annual conclusion to the Audit Committee for review and approval.

The Chief Internal Auditor will liaise with the external auditors on matters of mutual interest and to seek opportunities for cooperation in the conduct of audit work. The external auditors will have the opportunity to rely on the work of internal audit where appropriate.

A range of internal audit services are provided (Annex 1) in the delivery of the audit plan and to form the annual conclusion. The approach is determined by the Chief Internal Auditor and will depend on the level of assurance required, the significance of the objectives under review to the organisation's success, the risks inherent in the achievement of objectives and the level of confidence required that controls are well designed and operating as intended.

Fraud and irregularity

Internal audit will plan and evaluate their work to have a reasonable expectation of detecting fraud and identifying any significant weaknesses in internal controls.

Management is required to report all suspicions of theft, fraud and irregularity to the Chief Internal Auditor so that they can consider the adequacy of relevant controls, evaluate the implication of the fraud on the risk, control and governance processes and consider making recommendations as appropriate.

Internal audit will not carry out investigations unless commissioned to do so and where this is the case, the Chief Internal Auditor will ensure that investigators are appropriately trained in carrying out their responsibilities.

Where there is evidence that Council staff are committing fraud, internal audit will liaise with Human Resources and the Directorate concerned.

Internal audit will consider assurance over the Council's Anti-Fraud, Bribery and Corruption Strategy and framework as part of the internal audit planning process.

5. Internal audit resources

The Chief Internal Auditor is professionally qualified (CMIIA, CCAB or equivalent), maintains a comprehensive understanding of the Global Internal Audit Standards in the UK Public Sector, has wide internal audit and management experience, reflecting the responsibilities that arise from the need to build and manage an effective internal audit function (incl. recruitment, training and development), liaises internally and externally with Members, senior management and other professionals, and demonstrates sound sector knowledge & experience.

The Strategic Director of Corporate Resources will provide the Chief Internal Auditor with the resources necessary to fulfil the Council's requirements and expectations to fulfil the audit mandate and delivery of the internal audit strategy.

The Head of the Southern Internal Audit Partnership has a resource strategy in place to optimise internal audit resources. Ongoing sufficiency of resources (financial, human and technological) will be transparently communicated by the Chief Internal Auditor to the Executive Management Team and Audit Committee through regular reporting as part of the approval of the internal audit plan and further throughout the year as part of the progress reports and ultimately within the annual conclusion.

Any resource implications that put the fulfilment of the internal audit mandate at risk will be reported accordingly through the afore mentioned reports.

Financial Resource

The Head of Southern Internal Audit Partnership will manage the internal audit budget to enable the successful implementation of the internal audit strategy and achievement of the plan. The budget includes the resources necessary for the function's operation, including training and relevant technologies and tools.

The Head of the Southern Internal Audit Partnership will manage the day-to-day activities of the internal audit function effectively and efficiently, in alignment with the budget.

Human Resource

The Head of Southern Internal Audit Partnership will ensure that the internal audit service has access to an appropriate range of knowledge, skills, qualifications and experience required to deliver the internal audit strategy and operational risk-based audit plan.

The Chief Internal Auditor continually evaluates the competencies of individual internal auditors (regular one-to-ones, performance management and quality review processes), and encourages professional development.

The annual operational risk-based plan will identify the resources required to complete the work, thereby highlighting sufficiency of available resources. The Chief Internal Auditor can propose an increase in audit resource or a reduction in the number of audits if there are insufficient resources.

The Executive Management Team and Audit Committee will be advised where, for whatever reason, internal audit is unable to provide assurance on any significant risks within the timescale envisaged by the risk assessment process.

Significant matters that jeopardise the delivery of the plan or require changes to the plan will be identified, addressed and reported to the Executive Management Team and Audit Committee.

If the Chief Internal Auditor, Executive Management Team or the Audit Committee consider that the scope or coverage of internal audit is limited in any way, or the ability of internal audit to deliver a service consistent with the Global Internal Audit Standards in the UK Public Sector is prejudiced, they will advise the Strategic Director of Corporate Resources, accordingly.

Technological Resource

The Head of the Southern Internal Audit Partnership will ensure the internal audit function has technology to support the internal audit process and regularly evaluate the technology used to pursue opportunities to improve effectiveness and efficiency.

The implementation of new technologies is supported through effective and timely training for internal audit staff.

The impact of any technology limitations on the effective and efficient delivery of internal audit services will be communicated to the Executive Management Team and Audit Committee.

6. Ethics and Professionalism

The Chief Internal Auditor will ensure that internal auditors:

- Conform with the Global Internal Audit Standards in the UK Public Sector, including the principles of Ethics and Professionalism: integrity, objectivity, competency, due professional care, and confidentiality.
- Understand, respect, meet, and contribute to the legitimate and ethical expectations of the Council and be able to recognise conduct that is contrary to those expectations.
- Encourage and promote an ethics-based culture in the Council.
- Report organisational behaviour that is inconsistent with the Council's ethical expectations, as described in applicable policies and procedures.
- Apply the Seven Principles of Public Life alongside existing ethical frameworks.

7. Independence and objectivity

The Chief Internal Auditor retains no roles or responsibilities that have the potential to impair the internal audit functions independence, either in fact or appearance.

Should such circumstance arise, the Chief Internal Auditor will advise the Audit Committee of the safeguards put in place to manage actual, potential or perceived impairments.

Internal auditors will have no direct operational responsibility or authority over any of the activities they review.

Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, or engage in other activities that may impair their judgment, including:

- assessing specific operations for which they had responsibility within the previous year.
- performing operational duties for the Council or its affiliates.
- initiating or approving transactions external to the internal audit function.
- directing the activities of any Council employee that is not employed by the internal audit function, except to the extent that such employees have been appropriately assigned to internal audit team or to assist internal auditors.

Internal auditors will:

- disclose impairments of independence or objectivity, in fact or appearance, to the Chief Internal Auditor.
- exhibit professional objectivity in gathering, evaluating, and communicating information.
- make balanced assessments of all available and relevant facts and circumstances.
- take necessary precautions to avoid conflicts of interest, bias, and undue influence.

Induction and refresher training combined with internal audit procedures and guidance provide a systematic and disciplined approach for gathering and evaluating information to provide a balanced assessment of the activity under review.

The Chief Internal Auditor will ensure that the internal audit function remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication.

If the Chief Internal Auditor determines that objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively such that they believe in their work product, do not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance.

In addition, to achieve the degree of independence and objectivity necessary to effectively discharge its responsibilities, arrangements are in place to ensure the internal audit activity:

- operates in a framework that allows unrestricted access to the Executive Management Team and Audit Committee.
- reports functionally to the Audit Committee.
- reports in their own name.
- rotates responsibilities for audit assignments within the internal audit team.
- completes individual declarations confirming compliance with rules on independence, objectivity, conflicts of interest and acceptance of inducements, and
- ensures the planning process recognises, records and addresses potential conflicts of interest.

A register of potential conflicts of interest will be maintained with each case assessed and outcomes documented. If, despite this, independence or objectivity is impaired in fact or appearance, the details of the impairment will be disclosed to the Executive Management Team and Audit Committee. The nature of the disclosure will depend upon the impairment.

The Executive Management Team will ensure that independence is safeguarded through ensuring internal audit's access to staff and records, as set out in regulations and the charter, operates freely and without any interference and where there are actual or potential impairments to the independence of internal audit, the Executive Management Team will work with the Chief Internal Auditor to remove or minimise them or ensure safeguards are operating effectively.

The Audit Committee will support internal audit's independence by reviewing the effectiveness of safeguards at least annually, including any issues or concerns about independence raised by the Chief Internal Auditor.

The Chief Internal Auditor will confirm to the Audit Committee, at least annually, the organisational independence of the internal audit function. The Chief Internal Auditor will disclose to the Audit Committee any interference internal auditors encounter related to the scope, performance, or communication of internal audit work and results. The disclosure will include communicating the implications of such interference on the internal audit function's effectiveness and ability to fulfil its mandate

Matters around the appointment, removal, remuneration and performance evaluation of the Chief Internal Auditor will be undertaken by the Head of the Southern Internal Audit Partnership.

The Audit Committee should provide feedback on the performance evaluation of the Chief Internal Auditor. This will be achieved through an annual survey sent to all Audit Committee members.

8. Due Professional Care

Internal auditors will perform work with due professional care, competence and diligence. Internal auditors cannot be expected to identify every control weakness or irregularity, but their work should be designed to enable them to provide reasonable assurance regarding the controls examined within the scope of their review.

Internal auditors will have a continuing duty to develop and maintain their professional skills, knowledge and judgement based on appropriate training, ability, integrity, objectivity and respect.

Internal auditors will apprise themselves of the Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government and will work in accordance with them in the conduct of their duties.

Internal auditors will be alert to the possibility of intentional wrongdoing, errors and omissions, poor value for money, failure to comply with management policy and conflicts of interest. They will ensure that any suspicions of fraud, corruption or improper conduct are promptly reported to the Chief Internal Auditor in accordance with the Council's laid down procedures.

Internal auditors will treat the information they receive in carrying out their duties as confidential. There will be no unauthorised disclosure of information unless there is a legal or professional requirement to do so. Confidential information gained during internal audit work will not be used to effect personal gain.

9. Communication, Reporting and Oversight

Internal Audit Strategy

The Head of the Southern Internal Audit Partnership will develop and implement a strategy for the internal audit function that supports the strategic objectives and success of the Council and aligns with the expectations of the Audit Committee, Executive Management Team and other key stakeholders.

The internal audit strategy is a plan of action designed to achieve the audit function's long-term objective(s). The internal audit strategy includes a vision, strategic objectives, and supporting initiatives for the internal audit function to help fulfil the internal audit mandate.

Internal Audit Charter

The internal audit charter defines the internal audit function's mandate, organisational position, reporting relationships, scope of work, types of service, and other specifications relevant to its effective operation.

Audit Plan

The Chief Internal Auditor will develop an internal audit plan that supports the achievement of the Council's objectives.

The plan will be based on a documented assessment of the Council's strategies, objectives, and risks. Such assessment will be informed through engagement with the Audit Committee, and Executive Management Team as well as the Chief Internal Auditors understanding of the organisation's governance, risk and control processes.

The plan will be regularly reviewed with significant changes discussed and approved with the Executive Management Team and Audit Committee in a timely manner.

Audit Assignments

Internal auditors will communicate with management at the commencement of each review to ensure that the scope and timing of the work is understood and agreed, and this will be documented in a Terms of Reference. Internal audit contacts agreed as part of this process will be expected to be available for discussions and to provide the information required to complete the assignment in line with the timelines agreed. Regular communication throughout the review will ensure timely awareness of any issues arising and a close of audit meeting will also be held to summarise and confirm findings.

The results of all planned audit assignments will be summarised in a formal report, including:

- the purpose and scope of the reviews
- the assurance opinion
- an executive summary
- action plans outlining issues arising and actions proposed by management to address them (including consideration of root cause and identification of key themes).

The reports will be distributed and agreed in line with established reporting protocols for each Directorate.

Progress Reports

Throughout the year the Chief Internal Auditor will maintain regular communications with the Executive Management Team and Audit Committee on internal audit performance and other matters such as:

- revisions to the plan.
- any impairments to independence.
- significant risk exposures and control issues, including fraud risks, governance issues, and other areas of focus for management that could interfere with the achievement of the Council's strategic objectives.
- results of assurance and advisory services.
- management's responses to risk that the internal audit function determines may be unacceptable or acceptance of a risk that is beyond the Council's risk appetite.
- performance measures, including ongoing conformance with the Global Internal Audit Standards in the UK Public Sector.
- evaluation of resourcing to meet the requirements of the internal audit mandate / plan.

Annual Conclusion

The Chief Internal Auditor shall deliver an annual conclusion that can be used by the Council to inform its annual governance statement.

The annual conclusion will conclude on the overall adequacy and effectiveness of the Council's framework of governance, risk management and control.

The annual conclusion will incorporate as a minimum:

- the opinion.
- a summary of the work that supports the opinion.
- a statement on conformance with Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government.
- results of the quality assurance and improvement programme.

Quality assurance and Improvement Programme

The Head of the Southern Internal Audit Partnership maintains a quality assurance and improvement programme that covers all aspects of the internal audit function. The programme includes:

External Quality Assessments – to be performed at least once every five years by a qualified independent assessor or assessment team (with appropriate characteristics and sector knowledge). The requirement for an external quality assessment may also be met through a self-assessment with independent validation.

The decision on the appointment of the external assessor and format of the external quality assessment will be communicated to the Council's Executive Management Team and Audit Committee.

Internal Quality Assessments – self-assessments to be performed annually to review internal audits conformance with the Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government along with progress towards performance objectives.

The Chief Internal Auditor will communicate annually the results of the internal quality assessment to the Executive Corporate Management Team and Audit Committee. The results of external quality assessments will be reported when completed.

In both cases communications will include:

- The internal audit function's conformance with Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government and achievement of performance objectives.
- Compliance with laws and regulations relevant to internal auditing.
- If applicable, plans to address the internal audit function's deficiencies and opportunities for improvement.

In addition, an annual satisfaction survey will be conducted with key stakeholders to assess the value of the service and to seek suggestions for improvement.

The results of the survey, annual self-assessment, and external assessment will be shared with the Executive Management Team and Audit Committee, together with plans to address any issues arising.

Executive Management Team

As those responsible for the leadership and direction of the Council it is imperative that the Executive Management Team are engaged in:

- input, review and note the internal audit mandate and charter (minimum annually).
- input, review and note the internal audit strategy.
- Input and note the risk based internal audit plan (making appropriate enquiries of the Chief Internal Auditor to determine inappropriate scope and resource limitations).
- receiving regular progress reports from the Chief Internal Auditor on the outcomes and internal audits performance relative to its plan.
- review and note the Chief Internal Auditors annual conclusion.
- review of the quality assurance and improvement programme, engaging with, and receiving the results of internal and external assessments, including areas of non-conformance.

The Audit Committee

As those responsible for the governance of the Council it is imperative that the Audit Committee are engaged in:

- input, review and approval of the internal audit mandate and charter (minimum annually).
- input, review and note the internal audit strategy.
- input, and approval of the risk based internal audit plan (making appropriate enquiries of management and Chief Internal Auditor to determine inappropriate scope and resource limitations).
- receiving regular progress reports from the Chief Internal Auditor on the outcomes and internal audits performance relative to its plan.
- consider the Chief Internal Auditors annual conclusion.
- review of the quality assurance and improvement programme, engaging, with, and receiving the results of internal and external assessments, including areas of non-conformance.
- participation in discussions with the Chief Internal Auditor and senior management about the “essential conditions,” described in the Global Internal Audit Standards in the UK Public Sector.
- overview of significant advisory services not already included in the audit plan, prior to acceptance of the engagement.

10.Review of the internal audit mandate and charter

This mandate and charter will be reviewed annually (minimum) by the Chief Internal Auditor and reported to the Executive Management Team and Audit Committee for approval to ensure that any changes to the Global Internal Audit Standards in the UK Public Sector, reorganisation within the organisation or other significant changes affecting the nature and scope of internal audit services are considered.

Annex 1

Assurance Services

- **Risk based audit**: in which risks and controls associated with the achievement of defined business objectives are identified and both the design and operation of the controls in place to mitigate key risks are assessed and tested, to ascertain the residual risk to the achievement of managements' objectives. Any audit work intended to provide an audit opinion will be undertaken using this approach.

- **Developing systems audit**: in which the plans and designs of systems under development are assessed to identify the potential weaknesses in internal control and risk management; and programme / project management controls are assessed to ascertain whether the system is likely to be delivered efficiently, effectively and economically.

- **Quality assurance review**: in which the approach and competency of other reviewers / assurance providers are assessed in order to form an opinion on the reliance that can be placed on the findings and conclusions arising from their work.

- **Advisory services**: in which advice can be provided, either through formal review and reporting or more informally through discussion or briefing, on the framework of internal control, risk management and governance.

  The nature and scope of advisory services may be agreed with the party requesting the service, provided the internal audit function does not assume management responsibility. Opportunities for improving the efficiency of governance, risk management, and control processes may be identified during advisory engagements. These opportunities will be communicated to the appropriate level of management.

- **Data analytics:** is a process of assessing data to find trends, patterns or other insights. Internal auditors use data analytics to find and define risks, errors, and anomalies that could reveal deeper problems. The extended use of data analytics helps provide greater levels of assurance through analysis of a total population rather than traditional sampling methodologies.

- **IT Audit**: a specialist IT audit team are in place that are experienced in covering all aspects of established and emerging technologies. With IT underpinning a vast majority of how we function assurance in this area is crucial. To be able to provide a fully qualified team of IT audit specialists is a fundamental component of the audit offering.

- **Fraud and irregularity investigations**: Internal audit may provide specialist skills and knowledge to assist in or lead fraud or irregularity investigations, or to ascertain the effectiveness of fraud prevention controls and detection processes.

- **Value For Money:** is implicit in the vast majority of our internal audit work, however, value for money work can also be conducted through review of the optimal use of resources to achieve an intended outcome, and can be summarised as:
  - **Economy** – minimising the cost of resources used or required (inputs) – spending less
  - **Efficiency** – the relationship between the output from goods or services and the resources to produce them – spending well
  - **Effectiveness** – the relationship between the intended and actual results of public spending (outcomes) – spending wisely

- **Third party assurance:** the availability of objective assurance from other assurance providers will be considered in determining audit needs. Where internal audit needs to work with the internal auditors of other organisations, a practice which is expanding with the development of more organisational strategic partnerships, the roles and responsibilities of each party, as well as billing arrangements, will be clearly defined, agreed and documented prior to the commencement of work. Internal audit will also ensure awareness of and seek to place reliance on the work of other independent review bodies.

APPENDIX 2

Southern Internal Audit Partnership

Assurance through excellence and innovation

NEW FOREST DISTRICT COUNCIL
INTERNAL AUDIT PLAN 2026-27

Prepared by: Antony Harvey, Deputy Head of Southern Internal Audit Partnership

March 2026

Introduction

The mandate for internal audit in local government is specified within the Accounts and Audit [England] Regulations 2015, which states:

> *'5. (1) A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.'*

The scope of internal audit includes both assurance and advisory services covering the entire breadth of New Forest District Council ('the Council'), including all activities, assets, and personnel of the organisation.

The role of internal audit is that of an:

> *'Independent, objective assurance and advisory service designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes'.*

The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively.

The Council's response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation's objectives.

The aim of internal audit's work programme is to provide independent and objective assurance to management, the Executive Management Team and the Audit Committee, in relation to the business activities; systems and processes under review that:

- the framework of internal control, risk management and governance is appropriate and operating effectively; and
- risks to the achievement of the Council's objectives are identified, assessed and managed to a defined acceptable level.

Conformance with internal auditing standards

From 1 April 2025, the 'standards or guidance' in relation to internal audit are those laid down in the Global Internal Audit Standards, Application Note: Global Internal Audit Standards in the UK Public Sector and the Code of Practice for the Governance of Internal Audit in UK Local Government. The collective requirements shall be referred to as the Global Internal Audit Standards in the UK Public Sector.

Standard 8.4 [External Quality Assessment] requires internal audit providers to undergo an external quality assessment every five years. In September 2025 JC Training Ltd were commissioned to complete an external quality assessment of the Southern Internal Audit Partnership against the Global Internal Audit Standards in the UK Public Sector.

In considering all sources of evidence the external assessment team concluded:

'SIAP has achieved an excellent result of 'generally achieves' in this EQA in relation to the GIAS and Application Note. The IIA use the term 'general achievement' or 'general conformance' to indicate that "internal audit activities were performed in general conformance with the Global Standards."

I include a summary of SIAP's conformance to the GIAS, below. Overall, I believe that the team has achieved an excellent performance given its size, together with the breadth and depth of the benchmark established by the new GIAS.

I am delighted to confirm that SIAP fully achieves 46 of the 52 Standards and generally achieves the remaining six Standards. There are no partial conformances, or areas where the team do not conform with any Standards.

I have undertaken ten reviews of diverse internal audit functions using the (new) GIAS to date and **this result puts SIAP firmly within the top quartile and represents the highest level of achievement and conformance with the new GIAS that I have seen to date**.'

Summary of IIA Conformance	Standards	Does not Conform	Partially Conforms/ Achieves	Generally Conforms/ Achieves	Fully Conforms/ Achieves	Total
Purpose of Internal Auditing	N/A					N/A
Ethics and Professionalism	13				13	13
Governing the Internal Audit Function	9			3	6	9
Managing the Internal Audit Function	16			1	15	16
Performing Internal Audit Services	14			2	12	14
	52	0	0	6	46	52

Developing the internal audit plan 2026-27

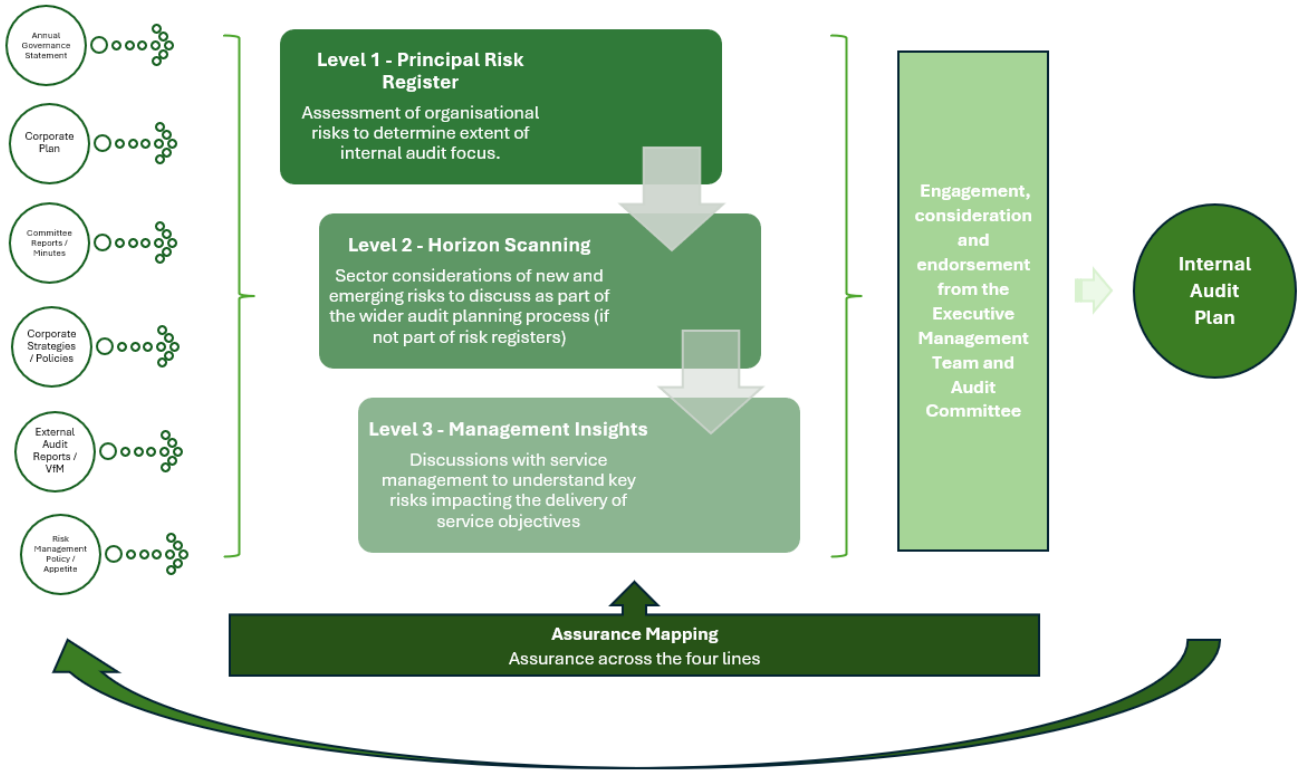
In accordance with the Global Internal Audit Standards in the UK Public Sector there is a requirement that internal audit must create a risk-based internal audit plan that supports the achievement of the organisation's objectives. The internal audit plan provides the mechanism through which the Chief Internal Auditor can ensure most appropriate use of internal audit resources to fulfil the audit mandate and delivery of the internal audit strategy.

The risk-based internal audit plan is prepared based on a range of inputs (see diagram).

Internal Audit focus should be proportionate and appropriately aligned. The plan will remain fluid and subject to on-going review and amendment, in consultation with the relevant audit sponsors, the Executive Management Team, and Audit Committee, to ensure internal audit are able to react to new and emerging risks and the changing needs of the Council.

Amendments to the plan will be identified through the Chief Internal Auditor's continued contact and liaison with those responsible for the governance of the Council and reported and approved by the Executive Management Team, and Audit Committee through regular progress reports.

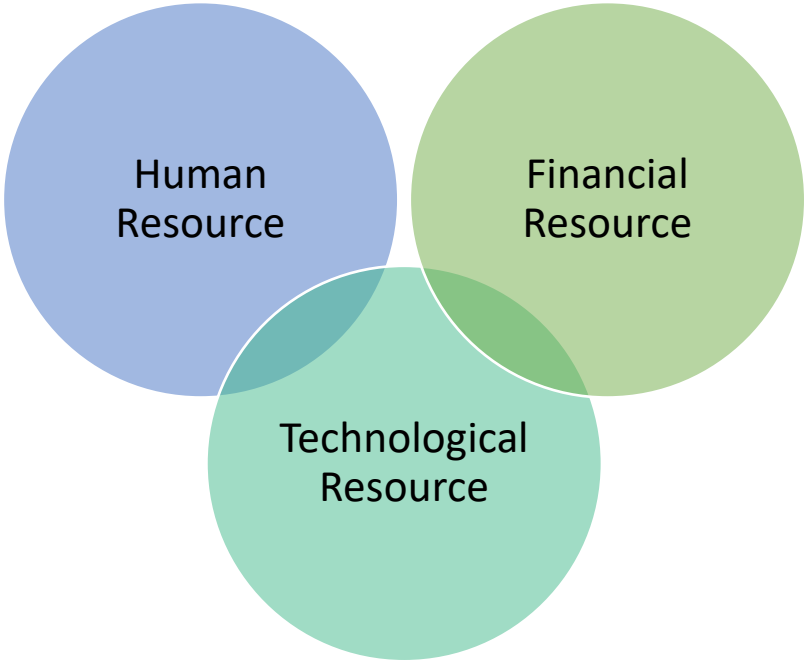
The Council are reminded that internal audit is only one source of assurance and through the delivery of our plan we will not, and do not seek to cover all risks and processes within the organisation. We will however continue to work closely with other assurance providers to ensure that duplication is minimised, and a suitable breadth of assurance is obtained.



Internal audit resources

On development of the 2026-27 internal audit plan as Chief Internal Auditor I am of the opinion that there is a sufficient level of resource available, supported by an appropriate range of knowledge, skills, qualifications and experience to deliver the internal audit plan in the fulfilment of the audit mandate and delivery of the internal audit strategy.

The Head of the Southern Internal Audit Partnership has a resource strategy in place to optimise internal audit resources to efficiently and effectively deliver the internal audit plan.



Human Resource - the internal audit service has access to an appropriate range of knowledge, skills, qualifications and experience required to deliver the internal audit strategy and operational risk-based audit plan.

If the Chief Internal Auditor, Executive Management Team or the Audit Committee consider that the scope or coverage of internal audit is limited in any way, or the ability of internal audit to deliver a service consistent with the Global Internal Audit Standards in the UK Public Sector is prejudiced, they will advise the Strategic Director of Corporate Resources, Section 151 Officer, accordingly.

Financial Resource - the Head of Southern Internal Audit Partnership will manage the internal audit budget to enable the successful implementation of the internal audit mandate and achievement of the plan. The budget includes the resources necessary for the function's operation, including training and relevant technologies and tools.

Technological Resource - the internal audit function has the technology to support the internal audit process and regularly evaluates technological resources in pursuit of opportunities to improve effectiveness and efficiency.

Resourcing the internal audit plan

The Global Internal Audit Standards in the UK Public Sector require a clear analysis of the resources and hours available for internal audit engagements compared to other administrative and non-audit related activities or initiatives focused on improving the internal audit function.

Activity			Days
Risk-Based Audit /Advisory	-	Delivery of risk-based internal audit assignments designed to fulfil the audit mandate, delivery of the internal audit strategy and in support of the Council in the achievement of their objectives.	320
Audit Management	-	Time allocated for the liaison and reporting to the Executive Management Team and Audit Committee, ongoing monitoring and update of the audit plan, implementation of management actions and ongoing quality review.	32
New Forest National Park Authority	-	Provision of audit days to fulfil the Council's Service Level Agreement with the National Park Authority	18
Total Audit Days	-	Total resource allocation for the delivery of the internal audit plan	370

*100% of the commissioned audit days are dedicated to fulfilling the audit mandate, and delivery of the internal audit strategy. Internal audit services are provided through the Southern Internal audit Partnership who undertake all administrative and non-audit related activities outside of the commissioned audit days.

A range of internal audit services are provided to deliver the internal audit plan (see Internal Audit Charter). The approach is determined by the Chief Internal Auditor and will depend on the level of assurance required, the significance of the objectives under review to the organisation's success, the risks inherent in the achievement of objectives and the level of confidence required that controls are well designed and operating as intended.

Your Internal Audit Team

Your internal audit service is provided by the Southern Internal Audit Partnership. The team will be led by Antony Harvey, Deputy Head of Southern Internal Audit Partnership (Chief Internal Auditor), supported by Jade Lakeland, Audit Manager.

Independence

The Chief Internal Auditor will ensure that the internal audit function remains free from all conditions that threaten the ability of auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. The Chief Internal Auditor is not aware of any relationships that may affect the independence and objectivity of the internal audit team.

The internal audit team retains no roles or responsibilities that have the potential to impair the internal audit functions independence, either in fact or appearance. Should such circumstance arise, the Chief Internal Auditor will advise the Audit Committee of the safeguards put in place to manage actual, potential or perceived impairments.

Internal Audit Plan 2026-27

The internal audit plan for 2026-27 is listed below and shows how the plan links to the Council's Corporate Plan Priority Themes, well as the principal risk register. The Council's three priority themes, underpinned by the Future New Forest transformation programme are as follows:

Underpinned by our Future New Forest transformation programme

Investing in our people and services to meet customer needs, protecting the council's financial position, and embedding sustainability through our Future New Forest transformation programme.

- Putting our customers at the heart of what we do
- Being an employer of choice
- Being financially responsible
- Designing modern and innovative services

Audit Assignment	Directorate Sponsor	Scope	Corporate Priority	Principal Risk Register Reference	Assurance / Advisory	Internal Audit Risk Assessment	Quarter
LGR/Devolution	ADT	Provision of days to respond to any Internal Audit requirements as a result of Local Government Reorganisation/Devolution.	All	PRR9	Assurance / Advisory	High	1-4
Corporate Governance Framework – AGS	ADS&E	To assess the framework for compiling the Annual Governance Statement (AGS) and monitoring action delivery with a focus on the new addendum, issued May 2025, applicable to the 2025-26 AGS.	All	PR8	Assurance	Medium	1
Information Governance – Data Breaches	SDCR	To provide assurance over the Council's arrangements to prevent, identify, investigate and learn lessons from data breaches.	All	PR6	Assurance	High	4
HR – Use of Agency staff, Interims and Consultants	SDCR	To assess the governance framework for utilising agency staff, interims and consultants to support the achievement of corporate priorities.	All	PR8, 9, 11, 13	Assurance	High	3
Cyber Incident Response Planning	ADT	Assurance over the plans in place to respond promptly and effectively to a cyber security incident to reduce the impact on Council services and data.	Transformation	PR1	Assurance	High	2
Vulnerability Management	ADT	Assurance over the policies, procedures and controls in place to identify and remediate vulnerabilities in the IT estate completely, promptly and effectively.	Transformation	PR1	Assurance	High	3-4

Audit Assignment	Directorate Sponsor	Scope	Corporate Priority	Principal Risk Register Reference	Assurance / Advisory	Internal Audit Risk Assessment	Quarter
Application Product Management	ADT	Assurance over the policies, procedures and controls in place to effectively manage applications including low code developments, e-forms, application upgrades.	Transformation	PR1	Assurance	Medium	3
Accounts Payable	SDCR	Regular assessment of core financial systems and processes.	Transformation	PR11, 12	Assurance	Medium	4
Income Collection and Banking	SDCR	Regular assessment of core financial systems and processes.	Transformation	PR11, 12	Assurance	Medium	3
NNDR	SDH&C	Regular assessment of core financial systems and processes.	Transformation	PR11, 12	Assurance	Medium	2
Housing Rents	SDH&C	Assurance over the arrangements to calculate and recover Housing Rents and service charges. The review will also assess/advise the Council with the preparations for implementation of the requirements of the new Rents Standards ahead of future Regulatory Inspections.	People	PR11 & SRR	Assurance / Advisory	High	1
Homelessness – Prevention & Relief	SDH&C	Assurance over the framework deliver strategic objectives and legislative requirements to prevent and relieve homelessness, including temporary accommodation placements.	People	PR3, 11, 20	Assurance	High	2
Housing Asset Management – Repairs and Maintenance	SDH&C	Following the implementation of the Maintenance and Repairs System (MARS),	People, Transformation	PR20 & SRR	Assurance	High	2

Audit Assignment	Directorate Sponsor	Scope	Corporate Priority	Principal Risk Register Reference	Assurance / Advisory	Internal Audit Risk Assessment	Quarter
		to provide over the governance, controls, and operational arrangements to repair and maintain the Council's housing stock.					
Housing Asset Management – Damp and Mould	SDH&C	Advisory role to assess the current governance, controls, and operational arrangements to prevent, identify, manage, and remediate damp and mould risks in its housing stock, protecting tenant health and meeting statutory and regulatory obligations (Awaab's Law). The review will inform potential developments in readiness for future RSH inspections.	People	PR20 & SRR	Advisory	High	1
Anti-Social Behaviour	SDH&C	To assess the arrangements for preventing and tackling Anti-Social Behaviour.	People	PR20, SRR	Assurance	Medium	2
Waste Collection	SDPOS	To provide assurance that the new waste collection service is operating in line with strategic objectives.	Place	PR14	Assurance	High	3
Trees – Inspection and Maintenance	SDPOS	To provide assurance that the Council have a complete inventory and robust arrangements to inspect and maintain trees on Council land.	Place	SRR	Assurance	High	2
Open spaces – Playground Safety	SDPOS	To assess the arrangements for the inspection and maintenance of play areas following a previous 'Limited Assurance' review.	Place	SRR	Assurance	High	3

Directorate Sponsor			
CX	Chief Executive	SDCR	Strategic Director Corporate Resources (S151)
COO	Chief Operations Officer / Deputy Chief Executive	SDPOS	Strategic Director Place, Operations & Sustainability
ADT	Assistant Director of Transformation	SDH&C	Strategic Director Housing & Communities
ADS&E	Assistant Director Strategy and Engagement (Monitoring Officer)		

Annexe 1

Contingency Reviews

The table below includes a list of engagements that would have been performed if additional resources were available.

Audit Assignment	Directorate Sponsor	Scope	Corporate Priority	Corporate Risk Register Reference	Assurance / Advisory	Internal Audit Risk Assessment	Quarter
Not Applicable. All reviews assessed as a high priority/risk have been incorporated into the plan.							

Included to enable the Audit Committee to assess the adequacy of resources available to the internal audit function.

Audit Committee – 27 March 2026

Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016

Purpose	For Review
Classification	Public
Executive Summary	This report provides Audit Committee with an update on the Council's use of its powers under the Regulation of Investigatory Powers Act 2000 ('RIPA') and the Investigatory Powers Act 2016 ('IPA'). It also includes an update on training provided to officers on RIPA and the IPA. Appended to this report is the recently updated Surveillance Policy for members to review to ensure that it is fit for purpose. This report also provides an update on the Council's current review by the Investigatory Powers Commissioner's Office ('IPCO').
Recommendations	**That Audit Committee:** **1. Notes the use made by the Council of its powers under RIPA and the IPA;** **2. Notes the update provided; and** **3. Endorses the Surveillance Policy.**
Reasons for recommendations	In accordance with the Surveillance Policy the Audit Committee should be updated on an annual basis on the Council's use of its powers under RIPA/IPA and should review the Council's policy to ensure that it is fit for purpose. This report ensures that the Audit Committee is so updated in accordance with these requirements.
Wards	All
Portfolio Holder	Councillor Jeremy Heron – Finance and Corporate

Strategic Directors	Alan Bethune – Strategic Director Corporate Resources (Section 151 Officer)
Officer Contact	Amanda Wilson Service Manager – Legal and Information Governance 02380 285306 amanda.wilson@nfdc.gov.uk

Introduction and background

1. The purpose of this report is to provide the Audit Committee with a summary of the Council's use of its powers under RIPA and the IPA.

2. RIPA and the IPA provide a statutory framework whereby certain surveillance and information gathering activities can be authorised and conducted by the Council in a lawful manner where they are carried out for the prevention and detection of crime and, in some cases, for the prevention of disorder.

3. When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights ('ECHR') enforceable in the UK.

4. Article 8 of the ECHR provides that individuals have the right to respect for private and family life and Article 6 of the ECHR provides that individuals have the right to a fair trial.

5. The use of covert surveillance techniques is considered to be an interference with this Article 8 right and therefore RIPA provides a framework to render lawful surveillance activities which might otherwise be in breach of the ECHR. It is also aimed at ensuring that evidence obtained against a person to be used in criminal proceedings is obtained in a fair manner.

6. There are three separate investigatory powers available to the Council, two of which are under RIPA:

   - Directed surveillance – which includes covert surveillance in public areas (not including residential premises or private vehicles, which is never permissible) which is likely to result in the obtaining of private information.

   - Use of Covert Human Intelligence Sources ('CHIS') – where a person establishes or maintains a personal or other relationship with a person for the covert purpose of using the relationship to

obtain information or to provide access to any information to another person or to covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. This includes undercover officers/ public informants.

And the third under the IPA:

- Obtaining communications data from telecommunications and postal operators – this includes service use or subscriber information (but not the content of a communication).

7. Before the Council may undertake these surveillance activities, there are various criteria which must be met including only carrying out covert surveillance where the criminal offence under investigation ordinarily carries a term of imprisonment of 6 months or more, its use is authorised internally by a senior officer (known as an Authorising Officer) and the external approval of the application by a Magistrate. Magistrates' approval also applies for the use and conduct relating to CHIS operatives.

8. For obtaining communications data under the IPA, authorisations involve scrutiny by the National Anti-Fraud Network, a body which acts as a Single Point of Contact on behalf of the Council to obtain external authorisation from the IPCO and obtaining the relevant data from communication providers.

9. The information obtained as a result of surveillance operations or acquired from telecommunications and postal operators can be relied on in court proceedings providing RIPA or the IPA is complied with.

The Council's use of RIPA and the IPA

10. The Council rarely uses its powers under RIPA and the IPA. The Council has not authorised any surveillance activities under RIPA or the IPA since the last report to the Audit Committee in March 2025, and members will note that no activity was recorded in the year before March 2025.

11. The Council provides a statistical return annually to the IPCO confirming its use of powers for the preceding calendar year. Accordingly, for 2025, this was a nil return.

IPCO Inspection

12. The IPCO provides independent oversight of all public authorities using covert investigatory powers under RIPA and the IPA. Its

statutory role includes ensuring that any use of surveillance, CHIS, or communications data is lawful, necessary and proportionate. As set out above, it also has a role in the approval process for the acquisition of communications data.

13. The IPCO also exercises robust inspection powers, granting inspectors access to systems, records and staff to review the full chain of decision-making and compliance. Inspection outcomes guide continuous improvement.

14. The IPCO's current approach is to no longer routinely undertake physical inspections of all local authorities. Instead, each local authority is required to provide a written update on its compliance with the legislation. Following the response to this written update, the IPCO will assess whether a further remote or on-site inspection is required.

15. The Council's last inspection was carried out in 2022. There were no areas of non-compliance identified. The inspection did identify several observations and recommendations to improve the Council's compliance.

16. On 10 July 2025, the IPCO wrote to the Council to request a written update. Officers have engaged with the IPCO, reviewed RIPA/IPA policies and documentation and taken steps to address the observations and recommendations previously made. A final update was provided to the IPCO on 4 March 2026. The Council is waiting to hear from the IPCO regarding the next steps.

Updated Surveillance Policy

17. Previously, the Council had separate policies for surveillance, comprising a directed surveillance policy, CHIS policy, and acquisition of communications data policy. The directed surveillance and CHIS policies were consolidated several years ago.

18. In keeping with the approach of other local authorities, and as part of the recent review, it was identified that it was appropriate to consolidate the acquisition of communications data policy into the principal Surveillance Policy.

19. The updated Surveillance Policy was agreed by the Council's Executive Management Team on 27 January 2026. This is included at **Appendix 1**. The updates to the Surveillance Policy include:

    - Reflecting the requirements of the current Home Office Codes of Practice issued under RIPA/IPA.
    - Additions regarding use of social media.

- Further guidance on non-RIPA surveillance activity.
- Changing the role of Senior Responsible Officer from the Chief Executive to the Council's Monitoring Officer.
- Updates to job titles of Authorising Officers.
- The requirement for Authorising and Investigating Officers to attend training every 2 years.

20. There is no change to the Council's approach to the powers available under RIPA and IPA and the existing governance arrangements in respect of these powers remain in place.

Training and awareness

21. In accordance with the Surveillance Policy all Authorising Officers and Investigating Officers should attend at least one training session every two years and further sessions as and when required.

22. Any officer contemplating the use of RIPA/IPA is required to seek advice from the Council's Legal Team prior to taking any action.

23. Over 40 employees with responsibilities related to RIPA/IPA, as Investigating Officers, Authorising Officers, or Legal Advisers were provided with training on RIPA/IPA and the Council's Surveillance Policy during January/ February 2026. This training is recorded centrally by the Legal Team and recorded on each employee's learning record.

24. Further training is due to take place in 2028.

25. Corporate awareness will be raised through annual updates being provided to all staff through the all staff communications email. The last update was provided on 6 March 2026.

Corporate plan priorities

26. The updated Surveillance Policy and steps taken to ensure compliance with RIPA and the IPA support the Council's Corporate Plan 2024 to 2028 for people, place and prosperity.

27. The steps taken support good governance and the Council's lawful approach to enforcement and keeping communities safe.

Consultation undertaken

28. The Executive Management Team were provided with an update on RIPA/IPA, and approved the updated Surveillance Policy, on 27 January 2026.

29. The Service Manager for Community Safety and Support was consulted on the CCTV elements of the Surveillance Policy.

Financial and resource implications

30. There are none arising directly from this report.

Legal implications

31. The Council must ensure that any use of investigatory powers under RIPA and the IPA is lawful, necessary, and proportionate, in line with statutory requirements and the Home Office Codes of Practice. Failure to comply may result in legal challenge, evidential issues in enforcement activity, and criticism from the IPCO, which has powers to inspect, review compliance, and issue recommendations.

32. An updated policy, regular training and reporting help maintain strong governance.

Risk assessment

33. A formal risk assessment is not deemed to be required.

Environmental / Climate and nature implications

34. There are none arising directly from this report.

Equalities implications

35. There are none arising directly from this report.

36. Enforcement activities to promote and protect the environment are undertaken by the Council but have not required the use of covert surveillance.

Crime and disorder implications

37. Ensuring compliance with RIPA and IPA safeguards strengthens the Council's ability to undertake lawful and proportionate enforcement activity, supporting effective prevention and detection of crime and disorder.

Data protection / Information governance / ICT implications

38. There are data protection implications associated with surveillance activity, as well as other enforcement activity. These are covered within the updated Surveillance Policy.

39. RIPA/IPA is designed to ensure that individual's rights to privacy are protected and interference with Article 8 rights under the EHCR is

limited by way of specific authorisation and in very specific cases. The Council's use of RIPA/IPA and understanding of the requirements supports the protection of individual rights.

Appendices:

Appendix 1–Surveillance Policy

Background Papers:

Published documents as referred to within report

This page is intentionally left blank

New Forest DISTRICT COUNCIL

Regulation of Investigatory Powers Act 2000 (“RIPA”)

Investigatory Powers Act 2016 (“IPA”)

Protection of Freedoms Act 2012

Human Rights Act 1998

Surveillance Policy

This Policy must be read in conjunction with the Home Office Codes of Practice

RIPA codes - GOV.UK

Communications data: code of practice - GOV.UK

Legal and Information Governance

Document publish date: 27 January 2026

Version number 1

Version	Author(s)	Date	Changes Made
1	Service Manager Legal and Information Governance	27 January 2026 (approved by EMT)	Conversion to new policy template, amalgamation of previous Surveillance and Acquisition of Communications Data Policies, updates.

Contents

1. Introduction

1.1 This policy sets out the statutory framework and procedures, including the relevant responsibilities of New Forest District Council ('the Council') and its officers, which govern the Council's lawful use of covert surveillance, covert human intelligence sources ('CHIS') and acquisition and disclosure of communications data for use in an investigation.

1.2 It is based on the requirements of:

- Regulation of Investigatory Powers Act 2000 ('RIPA'),
- Investigatory Powers Act 2016 ('IPA'),
- Home Office Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

  RIPA codes - GOV.UK
  Communications data: code of practice - GOV.UK

- Procedures and Guidance issued by the Investigatory Powers Commissioner's Office ('IPCO').

1.3 The use of covert surveillance, CHIS and the acquisition of service user or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law.

1.4 These powers should only be used in **exceptional circumstances**. RIPA requires that local authorities follow a clear authorisation process prior to using these powers.

1.5 Authorisations granted under Part II of RIPA or the IPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the Human Rights Act 1998 ('HRA').

2. Statutory Background

2.1 On 2 October 2000, the HRA came into force. This provides for fundamental rights and freedoms contained in the European Convention on Human Rights to be enforceable in UK Courts and Tribunals.

2.2 Article 8 of the Convention reads as follows:-

> *'Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others.'*

2.3 On 25 September 2000, RIPA came into force. This provides a lawful basis for 2 types of investigatory activity to be carried out by local authorities which might otherwise breach Article 8. The activities are:

- **directed surveillance**;
- covert human intelligence sources ("**CHIS**").

2.4 These surveillance techniques can **only** be authorised under RIPA where the use of the surveillance is necessary for the **prevention or detection of a crime** or (in some cases) for the **prevention of disorder**.

2.5 The IPA 2016 provides a lawful basis for local authorities to **acquire communications** data which was previously obtained through RIPA.

2.6 RIPA and IPA set out procedures that must be followed to ensure the surveillance and obtaining communications data activity is lawful which are set out in this policy.

2.7 All Investigating Officers and Authorising Officers should be familiar with RIPA, this Policy, the **Codes of Practice** issued by the Home Office, and the Procedures and Guidance issued by the IPCO.

3. Terminology

3.1 This section of the policy explains some of the terminology that is used in the context of surveillance activities.

Collateral Intrusion

3.2 Collateral Intrusion is the likely effect of the use of surveillance on the private and family life of persons who are not the intended subjects of the activity.

Confidential Information

3.3 This includes:

- Matters subject to legal privilege: Information relating to communications between a professional legal advisor and their client for the purposes of giving advice, in contemplation of legal proceedings or relating to legal proceedings.

- Confidential personal information: Information which relates to the physical or mental health, or spiritual counselling of a person (living or dead) who can be identified from it. For example, information about medical consultations/medical records.

- Confidential constituent information: Information relating to communications between a Member of Parliament and constituent in respect of constituency matters.

- Confidential journalistic information.

3.4 The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure.

3.5 Authorisation can only be granted by the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**).

Private Information

3.6 This includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationships with others, including family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and addresses.

3.7 Whilst a person may have a reduced expectation of privacy when in a public place, surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public. For example, two people holding a conversation on a public street or bus may have a reasonable expectation of privacy, even though they are in a public place.

3.8 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. For example, where an officer drives past a restaurant to take a photograph of the exterior, this is unlikely to require authorisation under RIPA, as the officer is not collecting private information. However, if the officer wishes to revisit the restaurant on a number of occasions to try to establish occupancy of the premises, this is likely to result in the obtaining of private information about the occupier, and authorisation for directed surveillance will usually be required.

Private vehicle

3.9 A private vehicle is any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company. This is distinct to vehicles owned or leased by public authorities.

Residential premises

3.10 Residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation.

4. Directed Surveillance

4.1 Directed surveillance is a form of surveillance activity that can be authorised under RIPA.

4.2 Surveillance generally includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- recording anything monitored, observed or listened to in the course of surveillance.
- surveillance with, or without, the assistance of a surveillance device.

Surveillance can be **overt** or **covert**.

4.3 Overt surveillance is surveillance which is not secretive or hidden i.e. it will be carried out openly. It includes surveillance where the subject has been told it will happen.

4.4 Covert surveillance is surveillance carried out in a manner calculated to ensure that subjects of it are unaware that it is or may be taking place.

4.5 Directed surveillance is a type of surveillance activity that can be authorised under RIPA. Directed surveillance is surveillance which is **covert** but **not intrusive** and is undertaken:

- For the purposes of a specific investigation or a specific operation
- In such a manner as is likely to result in the obtaining of **private information** about a person (whether or not one specifically identified for the purposes of the investigation or operation as detailed above) and
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance (for example if an officer happens to spot an offence taking place, they may stop and take

photographs as evidence, without requiring authorisation under RIPA).

4.6 Directed surveillance must also relate to the Council's **core functions** which are its specific public functions, rather than the ordinary functions that any organisation might have, for example HR functions.

4.7 Intrusive surveillance occurs when surveillance:

- is **covert**;
- relates to **residential premises** and/or **private vehicles**; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

4.8 Intrusive surveillance cannot be carried out or approved by the Council.

4.9 Following the changes to RIPA introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 a **crime threshold** applies to the authorisation of directed surveillance by local authorities.

4.10 Authorising Officers may not authorise directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND meets the following:

- The criminal offence is punishable by a maximum term of at least 6 months imprisonment; or
- Would constitute an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 (offences involving sale of tobacco and alcohol to underage children) regardless of length of prison term.

4.11 The crime threshold only applies to directed surveillance, not to CHIS or the acquisition of communications data.

Examples

4.12 It is possible to authorise directed surveillance under RIPA for some offences under the following categories which are relevant to the Council's functions:

- Fly tipping
- Benefit fraud
- Dangerous dogs
- Listed building offences

As the courts can impose a maximum term of at least six months' imprisonment.

4.13 Directed surveillance may only be carried out subject to the authorisation, approval at the Magistrates' Court and following the procedures in this policy.

4.14 The Home Office Code of Practice for covert surveillance can be found on the Home Office website at:

Covert surveillance code of practice - GOV.UK

4.15 Where covert surveillance is required but does not meet the RIPA crime threshold, or where it cannot fall under RIPA because it does not relate to the Council's core functions, a non-RIPA directed surveillance application may be made. Further details about surveillance outside of RIPA can be found at **Appendix 3** of this policy.

5. Covert Human Intelligence Sources ('CHIS')

5.1 The conduct and use of covert human intelligence sources (commonly known as an informant) occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person (i.e. if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose) or
- To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

5.2 The use and conduct of a CHIS may only be carried out subject to the authorisation, approval at the Magistrates' Court and following the procedures in this policy . This applies whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf.

5.3 Authorisation for CHIS can only be granted if it is for the purposes of 'preventing or detecting crime or of preventing disorder'.

5.4 If a CHIS is used, both the use of the CHIS and their conduct require prior authorisation.

- Conduct is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- Use includes actions inducing, asking or assisting a person to act as a CHIS.

5.5 Local authorities are not permitted to grant a CHIS to undertake criminal activity and no criminal conduct authorisations apply.

5.6 Members of the public who volunteer information to the Council in the ordinary course of business are not CHIS and do not require RIPA authorisation.

5.7 There may be instances where an individual, who covertly discloses information though not tasked to do so may nevertheless be a CHIS in accordance with section 26(8) (c) of RIPA. If they acquired the information in the course of, or as a result of the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS.

5.8 A relationship could exist even if only a single event takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the nature of that contact.

Examples:

5.9 The following **will not** be a CHIS:

- A member of the public volunteers a piece of information to the Council regarding something they have witnessed in their neighbourhood. They will not be a CHIS as they are not passing on information as a result of a relationship which has been established or maintained for a covert purpose.

- A person complains about excessive noise coming from their neighbour's house and the Council ask them to keep a noise diary. They will not be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose.

5.10 The following **will** be a CHIS:

- Intelligence received by the Council suggests that a local public house will sell alcohol to minors if they are familiar with them. A person under the age of 18 is engaged and trained by the Council and deployed to attend the licensed premises on a number of occasions and then try and purchase alcohol. In this situation a relationship has been established and maintained for the covert purpose and therefore a CHIS authorisation will be required.

- Without being asked, a person provides regular information to the Council about their neighbours' working hours and income as they believe their neighbour is committing benefit fraud. The person regularly visits their neighbour and engages in conversations about their work for the purpose of obtaining this information and passing it to the Council.

5.11 The use of a CHIS is the manipulation of a relationship to gain information. It is a higher risk covert technique and sufficient resources must be dedicated to the oversight and management of the operation.

5.12 The Home Office Code of Practice on Covert Human Intelligence Sources can be found on the Home Office website at:

Covert Human Intelligence Sources code of practice 2022 - GOV.UK

Vulnerable Individuals/ Juvenile CHIS

5.13 Vulnerable individuals and children (‘juveniles’) require greater care in regard to their safety and welfare when deployed as a CHIS.

5.14 Additional requirements, such as enhanced risk assessments, safeguards and protections, apply to the use of a vulnerable individual or a person under the age of 18 as a CHIS due to their level of understanding and/or age. In addition, the best interests of a child should be a primary consideration when deciding whether to deploy a child as a CHIS, during the operation and (if relevant) after the operation. The Council’s Safeguarding Policy should be considered and/or advice obtained prior to the CHIS application.

5.15 Both vulnerable adults and juvenile CHIS should only be used in exceptional circumstances and subject to the enhanced risk assessment process. Where appropriate, external advice should be sought when undertaking the enhanced risk assessment, for example from someone with relevant professional qualifications such as a social worker or an appropriately trained health professional.

5.16 In both cases authorisation for an application to the Magistrates Court can only be granted by the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**). Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the Council's Legal Team prior to making the application.

5.17 The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them. A juvenile CHIS who is aged 16 or 17 years old should only be deployed to gather information against a relative, their parents or any person who has parental responsibility for them where careful consideration has been given to whether the authorisation is justified in light of that fact. In such instances the rationale must be documented.

5.18 In other cases, authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

5.19 As with all CHIS activity, where the CHIS is a vulnerable adult or a juvenile, the requirements of the **Covert Human Intelligence Sources revised code of practice** must be complied with.

6. CCTV

6.1 The Council operates a close circuit television system ('CCTV') within certain towns in the New Forest District. Use of this system by the Council or third parties such as the police for directed surveillance would require authorisation under RIPA.

6.2 Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring public safety will not generally require RIPA authorisation, since the public will be aware that such systems are in use.

6.3 However, there may be occasions when the Council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required.

Examples:

- Overt CCTV cameras are used to gather information as part of a reactive operation (e.g. to identify individuals who have carried out flytipping). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.

- Covert CCTV cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people. A directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (e.g. a record of their movements and activities) and therefore falls within the definition of directed surveillance. The use of the CCTV cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

6.4 If another agency – e.g. the Police – wishes to use the Council's CCTV cameras for one of their investigations, this must be agreed by the Service Manager for Community Safety and Support or Operations Manager (CCTV). A copy of the other agency's RIPA authorisation form must be obtained and the details held with the Council's central register. In such circumstances, as long as there is a Police RIPA authorisation, there is no separate need for one of the Council's Authorised Officers to authorise the use of the cameras.

6.5 The deployment of mobile surveillance cameras is likely to be directed surveillance, requiring authorisation, where the surveillance of a specific person or group of people is intended. Requests for deployable CCTV should be made in accordance with the Council's CCTV Policy.

7. Acquisition and Disclosure of Communications Data

7.1 Communications Service Providers ('CSPs') are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also could include, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Council must obtain communications data from CSPs in strict compliance with IPA and the authorisation procedure set out in the policy.

Types of Communications Data

7.2 Communications data, telecommunications data and, postal data are defined in Sections 261 and 262 of IPA.

7.3 Communications data is the 'who', 'where', 'when' and 'how' of a communication and may relate to use of the following services:

- Postal service (anything comprised in or attached to a communication for the purpose of a postal service, for example addresses or markings of the sender or the recipient either in writing or through online tracking).
- Email.
- Landline telephone.
- Mobile telephone.
- Internet.

7.4 Telecommunications data are all communications data held by a telecommunications operator or obtainable from a telecommunications system. Under IPA, there are two types of telecommunication data:

- **Entity Data** - this is data about entities or links between individuals and devices. Entities can be individuals, groups and

objects such as mobile phones, tablets or other communication devices.

Entity data may include:

- names and addresses of subscribers, email or telephone account holders as well as payments made;
- make and model of the device used;
- the connection, disconnection and reconnection of services an individual has subscribed to or may have subscribed to.

Entity data describes or identifies how individuals are linked to devices but does not include information about individual events.

- **Events Data** - this is more intrusive; it identifies or describes events which consist of one or more entities, such as individuals engaging in an activity at a specific point (or specific points) in time.

Events data may include:

- call records;
- location of a mobile phone;
- information which identifies the sender or recipient from data held in the communication;
- timing and duration of a call.

Events data does not include non-communication events such as a change in address or telephone number.

Example of difference between entity and events data

7.5 Where an information check is required about who is the subscriber for a specific mobile number:

- The mobile number would be entity data;

- but if further information is required about the date/time a phone call was made by the subscriber, the location or the duration, this would be classed as events data.

7.6 The legal basis for obtaining events data is different than for entity data and must relate to 'serious crime' as defined in IPA, which is a higher threshold.

7.7 The **Home Office Communications Data Code of Practice** contains a list of examples of events data or entity data.

7.8 The Council is not permitted to make an application that requires the processing or disclosure of internet connection records for any purpose.

7.9 The Council is not able to intercept or obtain the content of communications in any circumstances, for example the details contained within an email, text message or voicemail.

Legal basis for Communications Data Authorisation and Notices

7.10 For the Council, the legal basis for the acquisition and disclosure of communications data is only for the prevention and detection of crime or disorder as set out in s73 and s60A IPA.

7.11 Obtaining events data must, in addition, be for 'a serious crime' defined in section 86(2A) IPA as:

- An offence for which an adult is capable of being sentenced to one year or more in prison;
- Any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- Any offence committed by a body corporate, or;
- Any offence which involves, as an integral part of it the sending of a communication or a breach of privacy.

7.12 Care should be taken that the appropriate lawful requirements for the purpose of the investigation are met and the correct authorisation procedure is followed before obtaining the data from communication service providers.

7.13 Acquisition and disclosure of communications data is also overseen by the Investigatory Powers Commissioner's Office (IPCO).

7.14 It is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority under section 11 IPA.

7.15 The Home Office Communications Data Code of Practice can be found on the Home Office website at:

Communications data: code of practice - GOV.UK

8. Online convert activity and use of Social Media

8.1 The internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public.

8.2 It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations.

8.3 If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

8.4 Where Council officers, or persons acting on the Council's behalf, conducts activity on the internet in such a way that they may interact with others in circumstances where the other parties could not reasonably be expected to know their true identity could require a CHIS authorisation. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites.

8.5 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered.

8.6 The Council's Social Media Policy should also be consulted.

8.7 Activity that does not meet the threshold for RIPA authorisation where private information is obtained will still require consideration of Human Rights issues, balancing the protection of rights with the breach of privacy, necessity and proportionality, as well as compliance with the Data Protection Act 2018.

8.8 Where the RIPA crime threshold is not met, a non-RIPA authorisation may still be required. Further information about non-RIPA can be found at **Appendix 3** of this policy.

Directed Surveillance:

8.9 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity.

8.10 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information.

8.11 Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

8.12 It is possible that when investigating one individual on social media/the internet you might obtain private information about other individuals not just the specific user on the profiles which are viewed, captured or recorded. These individuals might not even be aware this private information has been made public by the profile/account holder.

8.13 If reasonable steps are taken to inform the public or the subjects that surveillance could take place (where appropriate), the surveillance may be deemed as overt, for which authorisation may not be required.

8.14 If it is necessary and proportionate for an officer to breach access controls covertly, an authorisation for directed surveillance is required.

Example

- Where a public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation.

- When this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

8.15 In order to determine whether a directed surveillance authorisation should be sought, the following factors should be considered:

- Whether the investigation or research is directed towards an individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people;

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

- Whether the information obtained will be recorded and retained;

- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

CHIS

8.16 Where someone, such as an employee or member of the public, is tasked by the Council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the Council, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

8.17 Where a website or social media account requires a minimal level of interaction such as sending or receiving a friend request before access is permitted, this may not itself amount to establishing a relationship, nor would electronic gestures such as liking a post or following the subject's account as a reaction to information posted publicly. A directed surveillance application will still likely apply.

8.18 A CHIS authorisation should be considered if there is an intention to engage with posts covertly, or liking or following posts could lead to interaction with users. This could occur if an officer covertly asks to become a 'friend' of someone on social media where there is a private group.

8.19 It is not unlawful for an officer of the Council to set up a false identity, but an authorisation for the covert investigation would be required. Full consideration of the potential risks of such an approach should be considered at the outset and regularly reviewed.

Advice should be sought from the Legal Team on the covert use of the internet or social media as part of an investigation.

9. Authorisation Procedures

Directed Surveillance and CHIS

Roles of Investigation and Authorising Officers

9.1 Authorising Officers are responsible for assessing and authorising directed surveillance and the use of a CHIS.

9.2 Investigating Officers apply for authorisation from the Authorising Officers.

9.3 A full list of Authorising Officers and their responsibilities is shown in **Appendix 1**. Authorising Officers must not delegate their powers under RIPA.

9.4 A checklist for the respective duties of the Investigating Officer and the Authorising Officer is set out in **Appendix 2.**

9.5 Only Authorising Officers can authorise directed surveillance and the use of CHIS. All authorisations must follow the procedures set out in the policy. Authorising Officers are responsible for ensuring that they have received RIPA training prior to authorising RIPA activities.

9.6 It is the responsibility of Authorising Officers to ensure that when applying for judicial authorisation from the Magistrates' Court that the principles of necessity and proportionality are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

Necessity and Proportionality Test

9.7 Directed Surveillance and use of a CHIS can only be authorised if the Authorising Officer is satisfied that the activity is:-

- **in accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council, the Council's core functions.

- **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council

for authorising RIPA activity and there is a crime threshold for directed surveillance; and

- **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

9.8 Investigating Officers should ask the following questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the Article 8 of the Human Rights Act, or why the method proposed is justified.
- what other reasonable alternatives or less intrusive methods of obtaining information have been considered and why they have been discounted.

9.9 The risk of collateral intrusion should be risk assessed and what measures must be taken to avoid or minimise it. Particular care must also be taken in cases where confidential information is involved. In this instance, the only Authorising Officer will be the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**)

9.10 The Investigating Officer should take reasonable steps to risk assess and ensure that the person carrying out the surveillance or acting as a CHIS is clear on the scope of the activity, the conduct that is and is not authorised. The Investigating Officer and Authorising Officer should have due regard about how this will be managed during the covert operation.

9.11 Authorising Officers should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

9.12 A copy of the completed Home Office application and authorisation form must be forwarded to the Council's Legal Team within one week of the authorisation by e-mail as a scanned document. The Council's Legal Team will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

Role and Approval by Magistrates' Court

9.13 There is an additional stage in the process for RIPA Directed Surveillance and CHIS investigatory activities. After the authorisation form has been countersigned by the Authorising Officer, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

9.14 The magistrate will have to decide whether the Council's application to grant or renew an authorisation to use RIPA should be approved, and it will not come into effect unless and until it is approved by the Magistrates' Court.

9.15 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the RIPA surveillance techniques (i.e. Directed Surveillance and CHIS) at the same time.

9.16 In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation but could create an unnecessary administrative burden. Where the Council is not the lead authority, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

9.17 The role of the Magistrates' Court is set out in section 32A of RIPA. This provides that the authorisation, shall not take effect until the Magistrates' Court has made an order approving such authorisation. The matters on which the Magistrates' Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation was necessary and proportionate.
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
  - arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
  - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied.
- The local authority application has been authorised by an Authorising Officer;
- The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
  - 29(7)(a) (for CHIS),
  - 30(3) (for directed surveillance and CHIS).

The procedure

9.18 Investigating Officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant Home Office application form and forward it to the relevant Authorising Officer. The activity must be authorised before it takes place.

9.19 The following steps should be followed:

- Investigating Officer obtains preliminary legal advice from the Council's Legal Team.
- Investigating Officer completes the relevant Home Office application form.
- Authorisation is sought from the Authorising Officer.
- If the application is approved by the Authorising Officer, the Investigating Officer/ legal representative applies for Judicial approval, creates a court pack and Investigating Officer proceeds to court.
- Investigating Officer organises the directed surveillance or use of a CHIS to take place as set out within the parameters of the Court order.
- Investigating Officer sends copy of Magistrates' Court order to the Legal Team.

Additional Requirements for Authorisation of a CHIS

9.20 A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day-to-day responsibility for dealing with the CHIS (CHIS handler) and a senior Council officer with oversight of the use made of the CHIS (CHIS controller);
- a risk assessment has been undertaken to take account of the security and welfare of the CHIS;
- a Council officer is responsible for maintaining a record of the use made of the CHIS;

- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS.
- A record of decision for CHIS must be completed which covers the requirements that should be in place for handling a CHIS including juvenile and vulnerable CHIS.

Requirements for Authorisation of Acquisition and Disclosure of Communications Data

Roles

9.21 The rules on the granting of authorisations for the acquisition of communications data are different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:

- Investigating Officer;
- Approved Rank Officer;
- Senior Responsible Officer.

9.22 The two external roles are:

- Single Point of Contact (SPoC) at the National Anti-Fraud Network (NFAN);
- Authorising Officer in the Investigatory Powers Commissioner Office (IPCO).

9.23 **Investigating Officer** - This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data.

9.24 **Approved Rank Officer -** This is the Authorising officer who is aware that the application is being made by the Investigating Officer, and is able to verify to the SPoC at NAFN that the acquisition of communications data is necessary and proportionate for the purpose it is required for before it is authorised externally by IPCO.

9.25 **Senior Responsible Officer** - The Home Office Communications Data code of practice requires that local authorities must ensure that someone of at least the rank of the senior responsible officer (SRO) has overall oversight for obtaining Communications Data and must inform NAFN of nominated officers. The SRO for the acquisition and disclosure of communications data is the Council's Monitoring Officer.

9.26 **Single Point of Contact (SPoC) -** The accredited SPoCs at NAFN scrutinise the applications objectively and provide advice to Investigating Officers and Approved Rank Officers ensuring the Council acts in an informed and lawful manner. If no further work is required by the Council in respect of the application, the SPoC will refer the application to IPCO OCDA on the Council's behalf. SPoC's have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the Council, IPCO and the communication service providers.

9.27 **Authorising Officer at the Investigatory Powers Commissioners' Office (IPCO) -** Communications Data applications do not require judicial approval as is required for directed surveillance or CHIS under RIPA. The external Authorising Officer at the IPCO scrutinises the application independently and either approves or rejects the application setting out the justification for the decision, taking into account the lawfulness of the conduct, and that the appropriate standards and safeguards have been addressed. All correspondence about the application must be through the SPoC at NAFN.

The procedure for applying for Acquisition of Communications Data

9.28 The procedure is as follows:

- Investigating Officer obtains preliminary legal advice from the Council's Legal Team.

- Investigating Officer creates an application using the Cycomms Web Viewer on the NAFN website.
- SPoC Officer at NAFN triages and accepts the application into the Cyclops system.
- SPoC Officer uses Cyclops to update the application details and completes the SPoC report. As part of this, SPoC checks that the Council is lawfully permitted to obtain Communications Data for the purpose it is required for, determines the conduct such as the type of data needed to achieve the Council's purpose. Where the application is for Events Data, that the legal threshold is met and, in all cases, the conduct is justified based on the seriousness of the offence, the risk of unintended results, the risk of excessive data being obtained, including collateral intrusion, including whether other considerations or recommendations are required. The SPoC liaises with Investigating Officer and Approved Rank Officer if further work is required.
- SPoC sends the application to the IPCO for external approval on behalf of the Council.
- If SPoC receives authorisation from IPCO, SPoC sends request to CSP.
- SPoC receives results back from CSP and returns results to Investigating Officer (the applicant). Investigating Officer accesses the Web Viewer and downloads results.
- Investigating Officer sends details of the investigation, type of data required, whether the application was approved by IPCO and the date for this to the Council's Legal Team who will update the Central Record.

9.29 If the application is refused by IPCO, the Council can either:

- decide not to proceed with the application

- resubmit the application with revisions including the justifications for doing so
- challenge the decision made by IPCP if this is agreed by the SRO. Further guidance from IPCO can be provided.

Completing a Communication Data Application Form

9.30 An application to acquire communications data must:

- state the type of data required e.g., entity or events data; describe the communications data required e.g., the subscriber details linked to a telephone number, email address etc.;
- the timescales or specific date or period of the data that it is required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted;
- specify the purpose for which the data is required and set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder (or for events data, this must meet the threshold for serious crime).
  - include a unique reference number;
  - include the name and the office, rank or position held by the person making and verifying the application;
  - describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
  - include the operation name (if applicable) to which the application relates;
  - explain why the acquisition of that data is considered necessary and proportionate in the circumstances based on

the link between the investigation, the subject or other individuals, and why the specific communication data is required, what other lawful, reasonable or least intrusive methods were considered and why these were rejected;

- present the case for the authorisation in a fair and balanced way taking into account the size and scope of the investigation. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any risk of meaningful collateral intrusion. the extent to which the privacy rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it;

- consider and, where appropriate, describe any possible unintended consequences of the application; and

- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject/individual(s) of the fact that an application has been made for their data.

Urgent Authorisations (All covert activity)

9.31 As an authorisation under RIPA is not approved until signed off by a Magistrates' Court, urgent oral authorisations are not available.

9.32 Urgent oral authorisations are also not available for Communications Data.

10. Application Forms

10.1 The link to the Government application forms for Directed Surveillance and CHIS can be accessed from the link below:

RIPA forms - GOV.UK

10.2 For communications data, the application should be made electronically through the NAFN website.

10.3 The person completing the form is responsible for ensuring that the form used is the most up-to-date version

10.4 The forms for applications, renewals, reviews and cancellations should be completed in as much detail as possible.

10.5 Each investigation or operation should be given a unique reference number ('URN') on the application form by the Service Manager Legal and Information Governance. Any reviews, renewals or cancellation forms should be identified by the same URN.

Duration of the Authorisation

10.6 Authorisation/ notice durations are:

- for directed surveillance the authorisation remains valid for **3 months** after the date of authorisation;
- for a CHIS the authorisation remains valid for **12 months** after the date of authorisation (or **4 months** if a juvenile CHIS is used).
- a communications data notice remains valid for a maximum of **1 month**. All authorisations and notices are expected to specify dates and times for the acquisition or disclosure of the information.

10.7 Authorisations should not be permitted to expire; they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that **all** authorisations must be reviewed to decide whether to cancel or renew them.

Review of Authorisations

10.8 Authorising Officers must make arrangements to periodically review any authorised RIPA activity. It will be the responsibility of the Authorising Officer to diarise when reviews should be held.

10.9 Officers carrying out RIPA/ IPA activity, or external agencies engaged by the Council to carry out such activity on its behalf, must periodically review and report back to the Authorising Officer/ Approved Rank Officer if there is any doubt as to whether the activity should continue.

10.10 Reviews should take place as often as necessary and practicable, and this will need to be determined on a case by case basis. More frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information.

10.11 Where the nature or extent of the impact of an authorisation becomes greater than that anticipated in the original authorisation, the Authorising Officer should immediately review the authorisation and reconsider the proportionality of the operation.

10.12 For Juvenile CHIS, the CHIS Code of Practice stipulates that the authorisation should be reviewed on a monthly basis.

10.13 All reviews of RIPA activity should be recorded on the appropriate Home Office review form and must be sent to the Council's Legal Team within one week of the review to enable the central record on RIPA to be updated.

Renewal of Authorisations

10.14 If the Authorising Officer/ Approved Rank Officer considers it necessary for an authorisation to continue a renewal may be sought for a further period, beginning with the day when the authorisation would have expired but for the renewal. The Authorising Officer/ Approved Rank Officer must consider the matter again taking into account the content and value of the investigation and the information so far obtained.

10.15 Renewed authorisations will normally be for a period of:

- up to 3 months for directed surveillance,
- 12 months in the case of CHIS,
- 4 months in the case of juvenile CHIS and
- 1 month in the case of a communications data authorisation.

10.16 Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

10.17 Applications for the renewal of an authorisation for directed surveillance or CHIS authorisation must be made on the appropriate form and added as an addendum to the application form which granted the initial authorisation.

All directed surveillance and CHIS renewals will require an order of the Magistrates' Court.

10.18 A copy of the Council's notice of renewal of an authorisation must be sent to the Council's Legal Team within one week of the renewal, together with a copy of the Magistrates' Court order renewing the authorisation to enable the central record on RIPA to be updated.

10.19 For communications data, renewals must be made via the NAFN SPoC. The reasoning for seeking renewal of a communications data authorisation should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

Cancellation of Authorisations

10.20 The person who applied for or last renewed the authorisation must cancel it when they are satisfied that the directed surveillance, CHIS or communications data authorisation or notice no longer meets the criteria for authorisation, such as when it is no longer necessary for the statutory purpose or the activity is no longer deemed to be proportionate. For directed surveillance and CHIS cancellations must be made on the appropriate Home Office form.

10.21 Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters addressed.

10.22 A copy of the Council's notice of cancellation of an authorisation must be sent the Council's Legal Team within one week of the cancellation to enable the central record on RIPA to be updated.

10.23 For Communications Data, the NAFN SPoC must be made aware of the cancellation who will cease the authorised activity, ensure any notices are cancelled and inform the Communication Service Provider.

What happens if the surveillance interferes with the privacy of others?

10.24 Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases, the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and, in such cases, consideration should be given as to whether a separate authorisation is required.

11.Errors

11.1 An error should be reported if it is a ‘relevant error’ to IPCO.

11.2 Under section 231(9) of the IPA, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.

11.3 Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Code of Practice.

11.4 Where a relevant error has been identified, the Council should notify the IPCO as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO).

12.Records and Documentation

Departmental Records

12.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with another matter.

12.2 These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

12.3 In relation to communications data, records must also be held centrally by the SPoC. These records must be available for inspection by the IPCO and retained to allow the Investigatory Powers Tribunal to carry out its functions.

Central Record of Authorisations, Renewals, Review and Cancellations

12.4 A central record of directed surveillance, CHIS and access to communications data authorisations is maintained by the Council's Service Manager – Legal and Information Governance.

12.5 The central record is maintained securely in accordance with the requirements set out in the Home Office Codes of Practice. This is retained in perpetuity.

12.6 This will contain the following information:

- the type of authorisation
- the URN
- the dates that the authorisation was granted, reviewed, renewed or cancelled.
- details of attendances at the Magistrates' Court to include date of

- attendances, the determining Magistrate, the decision of the Court and the time and date of that decision.
- the name and rank of the Authorising Officer for the initial authorisation and any reviews, renewals or cancellations.
- whether the Authorising Officer is involved in the investigation.
- the file reference for the investigation.
- whether the authorisation was likely to result in the obtaining of confidential material.

12.7 In order to keep the central record up to date, Authorising Officers/Investigating Officers must, in addition to sending through the Home Office application, authorisation form, Magistrates' Court order or IPCO decision documents within one week of the authorisation being approved by the Magistrates' Court or IPCO, send notification (by e-mail) of every renewal, cancellation and review on the Council's notification forms within five working days.

12.8 In relation to the use of a CHIS the Services Manager Legal and Information Governance will also maintain the following documents:

- Any risk assessment in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.

12.9 Using the information on the central record the Council's legal Team will:

- remind Authorising Officers/Investigating Officers in advance of the expiry of authorisations;
- remind Authorising Officers and Investigating Officers of the need to ensure surveillance or CHIS conduct does not continue beyond the authorised period;
- remind authorising officers and Investigating Officers to regularly review current authorisations

- provide information to IPCO about the use of RIPA and IPA activity when required.

Safeguarding and the Use of Material (including Data protection considerations)

12.10 All material obtained through the use of directed surveillance, CHIS or acquisition of communications data records containing personal data must be handled in accordance with the Data Protection Act 2018 ('DPA') and the Council's Data Protection Policy.

12.11 The data protection principles under the DPA includes that personal data should only be processed if it is fair and lawful to do so, that the data processed are adequate, relevant and not excessive for the purpose it was collected.

12.12 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Care must also be taken that personal data collected as part of an investigation is held in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

12.13 A personal data breach may need to be reported to the Information Commissioner's Office within 72 hours of officers becoming aware of the breach

12.14 To mitigate against risk of personal data being compromised, all records and materials should be stored securely; clearly labelled; classified where appropriate as OFFICIAL or SENSITIVE to demonstrate the degree of sensitivity of the information; the appropriate retention period should be recorded at the outset and reviewed.

12.15 The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the HRA. Ensuring the continuity and integrity of evidence is critical to every prosecution.

12.16 Access to material obtained should be limited to those officers that have a legitimate reason for storing or accessing the records, with appropriate access controls in place. The data should not be stored for any longer than is necessary for any authorised purpose, and thereafter securely destroyed. This applies to all copies, extracts and summaries of the material obtained.

12.17 A record should also be made of all data pathways relating to material obtained through surveillance activities.

12.18 Where an authorisation results in excessive data having been acquired, the data should only be retained where it's appropriate and lawful to do so. The data must be reviewed to determine whether there is an intention to use it, and the reasons for requiring it, including whether retention of the data is necessary and proportionate. Contact the Legal Team if advice is required.

13. Governance, Oversight, and Continuous Compliance

Training and Awareness

13.1 The Service Manager – Legal and Information Governance will arrange regular training on RIPA and the acquisition of Communications Data.

13.2 All Authorising Officers and investigating officers should attend at least one session every two years and further sessions as and when required.

13.3 Any officer contemplating RIPA or the acquisition of Communications Data Should seek advice from the Council's Legal Team in the event of any queries or concerns as to the process.

13.4 The Service Manager – Legal and Information Governance will be responsible, along with the Senior Responsible Officer for raising corporate awareness of RIPA and this Policy.

Monitoring of Authorisations

13.5 The Monitoring Officer is the Senior Responsible Officer in relation to activity under RIPA and IPA and is responsible for:

- the integrity of the process in place to authorise directed surveillance, the use of a CHIS and the acquisition and disclosure of communications data
- compliance with Part II of RIPA, Part 3 of IPA, the relevant Home Office Codes of Practice and this Policy
- oversight of the reporting of errors to IPCO, and the identification of the causes of the errors and implementation of processes to minimise repetition of errors
- engagement with the Commissioner or Inspectors of the IPCO when they conduct inspections, and

- where necessary, overseeing the implementation of any post-inspection plans recommended or approved by the Commissioner
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection report prepared by the Commissioner.
- The IPCO has a duty to keep under review the exercise and performance of the Council's use of directed surveillance, CHIS, and the exercise and performance of the Council's use of its acquisition and disclosure of communications data powers. The IPCO will periodically inspect the Council and may carry out spot checks unannounced.

Complaints

13.6 Any person who believes they have been adversely affected by surveillance or other covert activity undertaken by or on behalf of the Council may complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Member review

13.7 The Service Manager – Legal and Information Governance will invite members every year through the Audit Committee to review the Council's RIPA Policy for that period to ensure it is fit for purpose. Members will also be provided with an annual update on the Council's use of its RIPA powers.

Policy and Implementation

13.8 This RIPA Policy is operational from { } and replaces any previous policies and procedures relating to RIPA, surveillance or acquisition of communications data.

Appendices

Appendix 1 - Functions that may be undertaken by Authorising Officers

1. Authorise an application for authority to carry out directed surveillance or for the conduct or the use of a CHIS.

2. Review an authorisation to carry out directed surveillance or the conduct or use of a CHIS on or before the specified date.

3. Authorise renewal of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

4. Authorise cancellation of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

5. Monitor the produce of the surveillance or from the conduct or use of a CHIS.

6. Authorise an application where the likely consequence of directed surveillance or conduct or use of a CHIS would be intrusion on another person other than the target (collateral Intrusion).

7. Authorise an application where the likely consequence of the directed surveillance or conduct or use of a CHIS would result in Council obtaining confidential material.

8. Authorise the use of a CHIS who is a minor.

9. Authorise the use of a CHIS who is a vulnerable person.

RANK/TITLE	**AUTHORISED FUNCTIONS (from numbered list above)**
Chief Executive	1-10
Deputy Chief Executive or a Strategic Director	1-7 (8,9, 10 in Chief Executive's absence)
Service Managers for: Development Management Environmental & Regulation Revenues, Benefits & Customer Services Public Realm & Sustainability Community Safety & Support Housing Resident Services	1-7

Appendix 2 Application and Authorisation Checklist

Investigating Officer must:

Read the Surveillance Policy document and be aware of any other relevant guidance.	
Determine that directed surveillance and/or a CHIS is required.	
For directed surveillance, assess whether the authorisation will be in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and be able to demonstrate that the suspected offence is subject to a custodial sentence of 6 months or more or that the surveillance is in connection with the sale of alcohol or tobacco to children.	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.	
Consider whether surveillance will be proportionate.	
Consider all less intrusive options which may be available and practicable and use that option first.	
If authorisation is necessary and proportionate, request a URN from the Service Manager Legal and Information Governance, prepare and submit an application to carry out directed surveillance or conduct or use of a CHIS to an Authorising Officer.	
REVIEW REGULARLY and submit to Authorising Officer on date set.	
If operation is no longer necessary or proportionate, complete cancellation form and submit to Authorising Officer.	

Authorising Officer must:

Consider in detail whether all options have been duly considered, including taking into account the Surveillance Policy document and any other relevant guidance.	
For directed surveillance, confirm that the offence is subject to a custodial sentence of 6 months or more or the surveillance is in connection with the sale of alcohol or tobacco to children.	
Consider whether surveillance can be considered to be in accordance with the law and is necessary and proportionate to the offence being investigated.	
Authorise only if an overt or less intrusive option is not practicable.	

Ensure the relevant judicial authority has made an order approving the grant of the authorisation.	
If surveillance is necessary and proportionate: • Review authorisation • Set review timetable	
Cancel authorisation when it is no longer necessary or proportionate.	

Appendix 3 Non-RIPA Guidance

1.1 Non-RIPA directed surveillance is covert surveillance:

- which does not meet the 'crime threshold' under RIPA 2000/ or the core function test and
- does not require external authorisation as under RIPA but instead requires internal authorisation.

1.2 Examples of non-RIPA surveillance could apply to matters which relate to civil matters such as some licensing matters, planning, safeguarding, immediate response surveillance or noise/anti-social behaviour investigations, debt recovery or matters where the RIPA lawful basis and 'crime threshold' (where relevant) is not met.

1.3 It must be noted that non-RIPA covert surveillance activity should only be undertaken where there is a lawful basis for doing so under Article 8 of the European Convention of Human Rights as set out in the HRA.

1.4 The use of non-RIPA should only be in exceptional circumstances and in line with the RIPA guidance set out for directed surveillance in this policy, and/or the use of a CHIS (where applicable). This includes the use of the internet and social media as part of covert investigations; further advice about the use of social media as part of investigations can be provided from the Legal Team if required.

1.5 The use of non-RIPA covert activity is high risk. If non-RIPA surveillance or other activity is deemed unlawful or not authorised or monitored correctly, the Council could be at risk of being the subject of complaints, the matter investigated by the Local Government and Social Care ombudsman, or result in legal or other action taken against the Council; all of which may result in reputational damage.

1.6 Case law has set out that the factors and procedure for non-RIPA surveillance should mirror the requirements under RIPA 2000 and the

Home Office statutory code of practice for covert surveillance as far as practicable.

1.7 This means that the Council is not permitted to undertake intrusive surveillance and higher levels of authorisation may be required for certain types of surveillance (e.g. obtaining certain types of confidential information).

1.8 Only Authorising Officers should authorise non-RIPA applications and renewals.

1.9 Investigating Officers should consult with the Council's Legal Team for preliminary advice on all proposed non-RIPA activity.

1.10 Investigating Officers and Authorising Officers should use the relevant RIPA forms which can be found on the intranet and mark these clearly as 'Non-RIPA directed surveillance'. Advice about completing the forms can be obtained from the Legal Team.

1.11 All non-RIPA Applications, authorisations, renewals and cancellations should be sent to Legal Team so that a record can be made on the central record. Where the use of the internet and social media is required as part of the investigation, the reasons for why the use of social media is required, how this will be undertaken, and the arrangements expected to be in place should be set out clearly.

1.12 Where the investigation may require a CHIS operative to set up or maintain a covert relationship for the purpose of obtaining information covertly or disclosing information which was obtained through such a relationship, a non-RIPA CHIS application may be required in addition to a non-RIPA directed surveillance application.

1.13 Applicants and Authorising Officers must be satisfied that covert activity under non-RIPA is lawful, necessary and proportionate in accordance with Article 8 of the ECHR as set out under the HRA.

1.14 The time period for authorisations and renewals should mirror the requirements under RIPA. Authorisations and renewals should not be allowed to expire.

1.15 Applicants must ensure all appropriate steps are taken to safeguard the material and that access to the information is on a 'need to know basis'. Where personal data is being processed, for example, the, use, handling and retention of materials, applicants must comply with all relevant data protection laws.

This page is intentionally left blank

AUDIT COMMITTEE

WORK PROGRAMME 2026/2027

ITEM	METHOD	LEAD OFFICER
26 JUNE 2026		
Draft Annual Financial Report 2024/25	Written Report	Alan Bethune/Paul Whittles
Procurement Contract Standing Orders, Breaches & Waivers 2025/26	Written Report	Josie West
Draft Annual Governance Statement 2024/25	Written Report	Alan Bethune/Matt Wisdom
Payment Card Industry Data Security Standard (PCI DSS) Update	Written Report	Alan Bethune/Paul Whittles
External Audit Plan for 2025/26	Written Report	Simon Mathers Rumana Ullah (External Audit)
Treasury Management Outturn Report 2025/26	Written Report	Gemma Farley Andrew Boutflower Daniel O'Rourke (HCC)
Annual Internal Audit Conclusion Report 2025-26	Written Report	Antony Harvey (Internal Audit)
Progress Update of Outstanding Management Actions	Written Report	Antony Harvey (Internal Audit)
Code of Good Governance Review Annual report	Written Report	Matt Wisdom

AUDIT COMMITTEE

WORK PROGRAMME 2026/2027

ITEM	METHOD	LEAD OFFICER
Annual Fraud Report 2025/26	Written Report	Ryan Stevens
Annual Report of Bad Debits and Write Offs	Written Report	Ryan Stevens
Principal Risk Register Review	Written Report	Josie West
30 OCTOBER 2026		
Housing Benefit Review Update	Presentation	KPMG
Audit Progress Report – Ernst & Young LLP	Presentation	Simon Mathers Rumana Ullah (External Audit)
Treasury Management Mid-Year Report 2026/27	Report	Daniel O'Rourke Gemma Farley Andrew Boutflower (HCC)
External Quality Assessment	Report	Antony Harvey (Internal Audit)
Internal Audit Progress Report 2026/27 (September 2026)	Report	Antony Harvey (Internal Audit)
Internal Audit Charter 2026/27 (September 2026)	Report	Antony Harvey (Internal Audit)

AUDIT COMMITTEE

WORK PROGRAMME 2026/2027

ITEM	METHOD	LEAD OFFICER
Risk Management Process	Report	Paul Whittles Karen Webber
29 JANUARY 2027		
Audit Results Report Year Ended 31 March 2026	Presentation	Simon Mather Rumana Ullah (External Audit)
Final Annual Financial Report 2024/25 Including Final Annual Governance Statement	Report	Paul Whittles
Auditors Annual Report Year Ended 31 March 2026	Report	Simon Mather Rumana Ullah (External Audit)
Internal Audit Progress Report 2026-27 (December 26)	Report	Antony Harvey (Internal Audit)
External Quality Assessment – Final Report	Report	Antony Harvey (Internal Audit)
Treasury Management Strategy 2027-2028 including Prudential Indicators	Report	Daniel O'Rourke (HCC)
Investment Strategy 2027/28	Report	Paul Whittles

AUDIT COMMITTEE

WORK PROGRAMME 2026/2027

ITEM	METHOD	LEAD OFFICER
Principal Risk Register		Karen Webber
19 MARCH 2027		
Internal Audit Progress Report 2025/26	Written Report	Antony Harvey (Internal Audit)
Internal Audit Plan and Charter 2026/27	Written Report	Antony Harvey (Internal Audit)
External Audit Plan	Written Report	Simon Mathers Rumana Ullah (External Audit)