

AUDIT AND GOVERNANCE COMMITTEE

AGENDA



Thursday 29 September 2022

at 2.00 pm

**in Committee Room B,
Civic Centre, Hartlepool**

MEMBERS OF AUDIT AND GOVERNANCE COMMITTEE:

Councillors Cook, Cowie, Creevy, Falconer, Feeney, Hall, Loynes, D Nicholson, Smith and Tiplady.

Standards Co-opted Independent Members: - Mr Martin Slimings and Ms Tracy Squires.

Standards Co-opted Parish Council Representatives: Parish Councillor John Littlefair (Hart) and Parish Councillor Alan O'Brien (Greatham).

Local Police Representative.

1. **APOLOGIES FOR ABSENCE**

2. **TO RECEIVE ANY DECLARATIONS OF INTEREST BY MEMBERS**

3. **MINUTES**

3.1 To confirm the minutes of the meeting held on 11 August 2022

4. **AUDIT ITEMS**

4.1 Treasury Management Strategy Update 2022/23 – *Director of Resources and Development*

4.2 Internal Audit Plan 2022/23 Update - *Head of Audit and Governance*

CIVIC CENTRE EVACUATION AND ASSEMBLY PROCEDURE

In the event of a fire alarm or a bomb alarm, please leave by the nearest emergency exit as directed by Council Officers. A Fire Alarm is a continuous ringing. A Bomb Alarm is a continuous tone.

The Assembly Point for everyone is Victory Square by the Cenotaph. If the meeting has to be evacuated, please proceed to the Assembly Point so that you can be safely accounted for.

5. OTHER ITEMS FOR DECISION

- 5.1 Regulation of Investigatory Powers Act 2000 (RIPA) – Annual Report (Including Quarter 1 Update) – *Chief Solicitor*

6. STANDARDS ITEMS

No items.

7. STATUTORY SCRUTINY ITEMS

Crime and Disorder Scrutiny

No Items

Health Scrutiny

- 7.1 Hartfield's Medical Practice (part of the McKenzie Group) – Closure:
- (a) Covering Report – *Statutory Scrutiny Manager (to follow)*;
 - (b) Engagement Outcome Update - Presentation - *McKenzie Group Practice and Tees Valley Clinical Commissioning Group*
 - (c) Verbal input from:
 - Councillors;
 - The MP for Hartlepool;
 - Healthwatch; and
 - Interested Groups / bodies. Residents.
- 7.2 Tees Valley Joint Health Scrutiny Committee – Outside Body Resignation – *Chief Solicitor and Monitoring Officer*

8. MINUTES FROM THE RECENT MEETING OF THE HEALTH AND WELLBEING BOARD

No items.

9. MINUTES FROM THE RECENT MEETING OF THE FINANCE AND POLICY COMMITTEE RELATING TO PUBLIC HEALTH

No items.

10. MINUTES FROM RECENT MEETING OF TEES VALLEY HEALTH SCRUTINY JOINT COMMITTEE

No items.

11. MINUTES FROM RECENT MEETING OF SAFER HARTLEPOOL PARTNERSHIP

No items.

12. REGIONAL HEALTH SCRUTINY UPDATE

No items.

13. DURHAM, DARLINGTON AND TEESSIDE, HAMBLETON, RICHMONDSHIRE AND WHITBY STP JOINT HEALTH SCRUTINY COMMITTEE

No items.

14. ANY OTHER BUSINESS WHICH THE CHAIR CONSIDERS URGENT

For information: -

Forthcoming Meetings: -

Thursday 10 November, 2022 at 10.00 am

Thursday 15 December, 2022 at 10.00 am

Thursday 12 January, 2023 at 10.00 am

Thursday 9 February, 2023 at 10.00 am

Thursday 16 March, 2023 at 2.00 pm

All meetings will take place at the Civic Centre, Hartlepool.

AUDIT AND GOVERNANCE COMMITTEE

MINUTES AND DECISION RECORD

11 AUGUST 2022

The meeting commenced at 10.00 am in the Civic Centre, Hartlepool

Present:

Councillor: Rob Cook (In the Chair)

Councillors: Cowie, Falconer, Feeney, Hall, Loynes, D Nicholson and Smith

Co-opted Members:

Martin Slimings and Tracy Squires – Independent Members
Parish Councillor Alan O'Brien (Greatham)

Also Present:

In accordance with Council Procedure Rule 4.2 Councillor Ben Clayton was in attendance as substitute for Councillor Rachel Creevy

Councillors Gordon Cranney and Sue Little

Officers: Hayley Martin, Chief Solicitor
Neil Wilson, Assistant Chief Solicitor
Chris Little, Director of Resources and Development
Noel Adamson, Head of Audit and Governance
Sylvia Pinkney, Assistant Director, Regulatory Services
Joan Stevens, Statutory Scrutiny Manager
Denise Wimpenny, Principal Democratic Services Officer

18. Apologies for Absence

Apologies for absence were submitted on behalf of Councillors Creevy and Tiplady, Parish Councillor John Littlefair (Hart) and Christopher Akers-Belcher, Chief Executive, Healthwatch.

19. Declarations of Interest

Councillor Leisa Smith declared a prejudicial interest in Minute 22 and indicated that although she was in attendance at the meeting, she would not be taking part in the decision making element.

20. Minutes of the meeting held on 7 July 2022

Confirmed.

21. Local Government (Access to Information) (Variation Order) 2006

Under Section 100(A)(4) of the Local Government Act 1972, the press and public were excluded from the meeting for the following item of business on the grounds that it involved the likely disclosure of exempt information as defined in the paragraphs referred to below of Part 1 of Schedule 12A of the Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) Order 2006.

Minute 22 – Council Referral – Councillor Gordon Cranney Investigation Report – This item contains exempt information under Schedule 12A of the Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) Order 2006 namely, information relating to any individual (para 1).

22. Council Referral – Councillor Gordon Cranney Investigation Report

(Chief Solicitor) This item contains exempt information under Schedule 12A Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) Order 2006 namely (para 1) information relating to any individual.

The Assistant Chief Solicitor reported on the findings of the investigation following the referral from Council on 25 May 2022 in relation to the conduct of Councillor Gordon Cranney, details of which were set out in the exempt section of the minutes. The Committee considered the report, the detail of which was included in the exempt section of the minutes.

Recommended

Details were set out in the exempt section of the minutes.

Further to discussions in the closed session of the meeting, the meeting returned to open session where the following agenda items were considered.

23. Letter to Those Charged with Governance – Compliance with Laws and Regulations/Fraud (*Director of Resources and Development*)

The Head of Audit and Governance submitted for the Committee's approval a letter to Mazars from the Chair of the Committee detailing how the Committee had complied with the requirements of International Standards for Auditing.

Recommended

That the contents of the letter to Mazars, outlining how the activities of the Committee had complied with the requirements of International Standards for Auditing be approved.

24. Internal Audit Outcome Report 2021/22 (*Head of Audit and Governance*)

The report provided Members with the Head of Audit and Governance assurance opinion on the adequacy and effectiveness of the Council's internal control environment and set out the outcomes of audit work for the period April 2021 to March 2022. There were 1085 audit days allocated to planned and responsive activities during 2021/22. Staffing resources were as anticipated and, although the level of support provided by internal audit to the COVID-19 response was slightly greater than anticipated, the internal audit section was still able to review all high risk functions and a balanced programme of work covering all Council departments in 2021/22.

The Head of Audit and Governance stated that based on the work undertaken during the year 2021/22, the opinion had been reached that reliance could be placed on the adequacy and effectiveness of internal controls operating across the Council in 2021/22. As reported in last year's opinion, those school audits that had not been undertaken as part of the 2020/21 internal audit plan had now been completed as part of the internal audit work in 2021/22.

Recommended

That the contents of the report be noted.

25. Role of the Chief Finance Officer (CFO) in Public Service Organisations (*Director of Resources and Development*)

The Head of Audit and Governance informed the Committee of the CIPFA statement – 'The Role of the CFO in Public Service Organisations', and how the Council complied with this guidance. It was highlighted that the Director of Resources and Development was also the Council's nominated Section 151 Officer. Members were referred to Appendix A of the report

which detailed how the Council ensured that the requirements of the statement were met.

The Director of Resources and Development responded to issues raised by Elected Members arising from the report including clarification around the definition of ‘value for money’, governance and audit arrangements as well as the checks in place to ensure satisfactory compliance.

Recommended

The Committee noted that the Director of Resources and Development had reviewed the CIPFA statement – ‘The Role of the CFO in Public Service Organisations’ and advised Members that the Council complied with these requirements, as detailed in Appendix A to the report.

26. Role of the Head of Internal Audit in Local Government *(Director of Resources and Development)*

The report informed the Committee of the CIPFA statement – “The Role of the Head of Internal Audit in Local Government”, and within the report demonstrated how the Council complied with this guidance. Members were referred to Appendix A of the report which detailed how the Council ensured that the requirements of the statement were met.

Recommended

The Committee noted that the Director of Resources and Development had reviewed the CIPFA statement – “The Role of the Head of Internal Audit in Local Government” and advised the Committee that the Council complied with these requirements as detailed in Appendix A to the report.

27. Annual Governance Statement 2021/22 *(Director of Resources and Development)*

The Head of Audit and Governance presented the Annual Governance Statement 2021/22, a copy of which was appended to the report, as required under the Accounts and Audit Regulations (England) 2015 for the Committee’s approval.

Recommended

That the submitted Annual Governance Statement 2021/22 be approved.

28. The 2021/22 Financial Report (including the 2021/22 Statement of Accounts) *(Director of Resources and Development)*

The Director of Resources and Development reported on the arrangements for approving the Council's financial report for 2021/22 including the Statement of Accounts, a copy of which was attached at Appendix A. The deadline for completion of the final audited accounts had been extended from 30 September to 30 November 2022 for this year only, the background to which was provided.

The Director highlighted the unprecedented financial impact on the Council as a result of the Covid pandemic and increased inflation pressures in terms of additional costs and reduced income, details of which were provided as set out in the report. The Council faced significant budget deficits and work had commenced to quantify the level and impact of inflationary pressures on the current year budget and this would be reported as part of the first quarterly review. The final revenue outturn position was a net underspend of £0.286m after earmarking of reserves for specific purposes. The underspend had been allocated to the Budget Support Fund. A detailed outturn report had been presented to Finance and Policy Committee on 26 July 2022, a summary of which was provided.

In the discussion that followed the Director of Resources and Development responded to queries raised arising from the report. Clarification was provided in relation to the balance sheet calculations, the impact of the pandemic on the Council's financial position including business rate collections as well as the reasons for adverse variances in expenditure.

Recommended

- (i) That the report and comments of Members be noted.
- (ii) That the Draft Financial Report detailed in Appendix A would be subject to independent audit by Mazars and details of any material amendments would be reported to Audit and Governance Committee later in the year.
- (iii) It was noted that there was the opportunity to raise questions and/or seek clarification of information included in the pre-audit Financial Report.

29. Safer Hartlepool Partnership Performance – Quarter 3 - October to December 2021 *(Director of Neighbourhoods and Regulatory Services)*

Purpose of report

To provide an overview of the Safer Hartlepool Partnership performance for Quarter 3 – October to December 2021 against key indicators linked to the priorities outlined in the draft Community Safety Plan 2021/24.

30. Safer Hartlepool Partnership Performance – Quarter 4 – January to March 2022 *(Director of Neighbourhoods and Regulatory Services)*

Purpose of report

To provide an overview of the Safer Hartlepool Partnership performance for Quarter 4 – January to March 2022 (inclusive) against key indicators linked to the priorities outlined in the Community Safety Plan 2021/24.

Issue(s) for consideration

The report provided an overview of the Partnership's performance during Quarters 3 and 4, as set out in appendices to the reports. Information as a comparator with performance in the previous year was also provided. In presenting the report, the Assistant Director, Regulatory Services highlighted salient positive and negative data and responded to queries in relation to crime figures by type.

The Chair questioned the figures in relation to the reduction in fly tipping and, given the perception that fly tipping was continuing to increase, suggested that this decrease be publicised.

The Chair raised a number of concerns in relation to the increase in deliberate fires particularly in certain wards within the town, and the impact as a result and requested more detailed information in terms of the locations of these incidents, to whom they had been reported as well as actions taken. The Assistant Director, Regulatory Services agreed to provide this information following the meeting.

Decision

- (i) That the contents of the report and comments of Members be noted.
- (ii) That the reduction in fly tipping be publicised.

- (iii) That a breakdown of figures in relation to locations of deliberate fires, to whom they had been reported and actions taken be provided following the meeting.

31. Date and Time of Next Meeting

The Chair reported that the meeting would be held on Thursday 8 September 2022 at 10.00 am.

The meeting concluded at 12.25 pm.

CHAIR

AUDIT AND GOVERNANCE COMMITTEE

29th September 2022



Report of: Director of Resources and Development

Subject: TREASURY MANAGEMENT STRATEGY UPDATE
2022/23

1. PURPOSE OF REPORT

1.1 The purposes of the report are to:

- i) Provide a review of Treasury Management activity for 2021/22 including the 2021/22 outturn Prudential Indicators; and
- ii) Provide the first quarter update of the 2022/23 Treasury Management activity.

2. BACKGROUND

2.1 The Treasury Management Strategy covers:

- the borrowing strategy relating to the Council's core borrowing requirement in relation to its historic capital expenditure (including Prudential Borrowing);
- the borrowing strategy for the use of Prudential Borrowing for capital investment approved as part of the Medium Term Financial Strategy; and
- the annual investment strategy relating to the Council's cash flow.

2.2 The Treasury Management Strategy needs to ensure that the loan repayment costs of historic capital expenditure do not exceed the available General Fund revenue budget. Similarly, for specific business cases the Treasury Management Strategy needs to ensure loan repayment costs do not exceed the costs built into the business cases. As detailed later in the report these issues are being managed successfully.

2.3 The Local Government Act 2003 requires the Council to 'have regard to' the CIPFA (Chartered Institute of Public Finance and Accountancy) Prudential Code and to set prudential indicators for the next three years to ensure capital investment plans are affordable, prudent and sustainable.

2.4 The Act also requires the Council to set out a Treasury Management Strategy for borrowing and to prepare an Annual Investment Strategy, which sets out the policies for managing investments and for giving priority to the

security and liquidity of those investments. The Secretary of State has issued Guidance on Local Government Investments which came into force on 1st April, 2004, with subsequent updates.

2.5 The Council is required to nominate a body to be responsible for ensuring effective scrutiny of the Treasury Management Strategy and policies, before making recommendations to full Council. This responsibility has been allocated to the Audit and Governance Committee.

2.6 This report covers the following areas:

- Economic background and outlook for interest rates;
- Treasury management outturn position for 2021/22; and
- Treasury Management Strategy 2022/23 first quarter review.

3. ECONOMIC ENVIRONMENT AND OUTLOOK FOR INTEREST RATES

3.1 **UK** – The UK economy has faced an extended and ongoing period of economic uncertainty due to the Covid-19 pandemic, and latterly significant inflationary pressures. The Bank of England's Monetary Policy Committee (MPC) have stated they have prioritised the dampening down of inflation pressures, even if it comes at the cost of sluggish growth, or, indeed recession. The market is pricing in Bank Rate increasing to 3.5% by April 2023.

3.2 The latest CPI data shows that the UK is at a new 40 year high of 10.1% (July). Economists had been forecasting CPI inflation would probably rise to 12.0% in October, with a risk of future increasing in the following months. The announcement by the Government of measures to cap prices will reduce pressure on inflation and the position will be assessed when more information available.

3.3 The Office for Budget Responsibility's revised growth forecast up to 2026 are set out in the following table, however, these will be revised at the next budget:

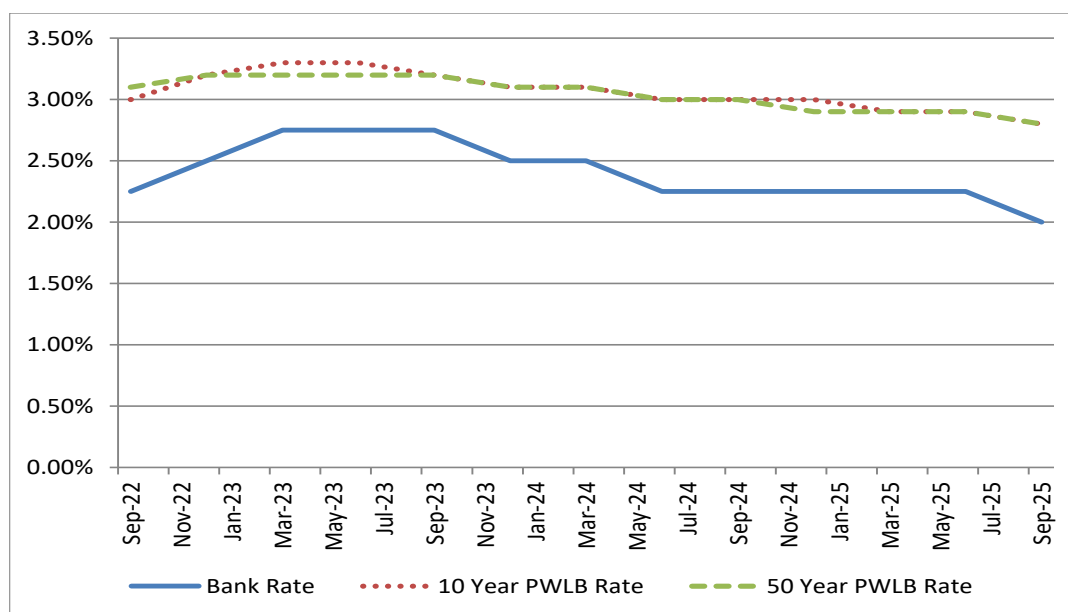
Year	March 2022 Growth Forecast
2022	3.8%
2023	1.8%
2024	2.1%
2025	1.8%
2026	1.7%

3.4 **European Union (EU)** – The euro-zone reached 8.9% inflation in July and in line with the Governing Council's strong commitment to its price stability mandate, they took further key steps to make sure inflation return to its 2% target over the medium term.

- 3.5 **Other Economies** – elsewhere economies are grappling with similar inflationary pressures and uncertainty caused by geopolitical events including the war in Ukraine and increasing tension between China and Taiwan. Central banks are responding with increases in bank rates, the USA Federal Reserve raising its benchmark interest rate by 0.75% in July, the second time it has done so in two months. Such measures are having a dampening effect on the world economy.

Interest Rate Forecasts

- 3.6 Link Asset Services (the Council's Treasury Management advisors) continue to update their interest rate forecasts to reflect statements made by the Governor of the Bank of England and changes in the economy.
- 3.7 In August the MPC increased the Base Rate by 0.5% to 1.75% pushing borrowing costs to the highest level since 2009. Forecast reflects a view that the MPC will be keen to further demonstrate its anti-inflation credentials by delivering additional increases in Bank Rate at future meetings. Link Asset Services forecast that the Bank Rate will peak at 2.75%, whilst the market is pricing in Bank Rate at 3.5% by April 2023. Link Asset Services fully accept there is potential risk to this projection.
- 3.8 The CPI measure of inflation is already at 10.1% and the Bank of England anticipates it will peak near 11% just before Christmas. With the cost-of-living squeeze and unemployment increasing, they predict that the Bank will pause following its March 2023 meeting and judge it has done enough so long as inflation starts to fall, albeit at a slow pace. They envisage the MPC waiting a full year before loosening the reins and starting to cut Bank Rate in Spring 24.
- 3.9 Economic and interest rate forecasting remains difficult with so many influences impacting on the economy. UK gilt yields (i.e. Government borrowing) and PWLB rates forecasts made by Link Asset Services, (and MPC decisions) may be liable to further amendment depending on how the political and economic developments transpire over the next year.
- 3.10 Link Interest Rate Forecast up to September 2025 are shown below:



- 3.11 Since the late 1990s Base Rate averaged 5% until 2009 when the Bank of England reduced it to historically low levels. Over the same period PWLB rates have been significantly higher than they are at present.

4. TREASURY MANAGEMENT OUTTURN POSITION 2021/22

Capital Expenditure and Financing 2021/22

- 4.1 The Council's approved capital programme is funded from a combination of capital receipts, capital grants, revenue contributions and prudential borrowing.
- 4.2 Part of the Council's treasury management activities is to address the prudential borrowing need, either through borrowing from external bodies, or utilising temporary cash resources within the Council. The wider treasury activity also includes managing the Council's day to day cash flows, previous borrowing activities and the investment of surplus funds. These activities are structured to manage risk foremost, and then to optimise performance.
- 4.3 Actual capital expenditure forms one of the required prudential indicators. As shown at Appendix A, the total amount of capital expenditure for the year was £18.555m, of which £7.411m was funded by Prudential Borrowing.
- 4.4 The Council's underlying need to borrow is called the Capital Financing Requirement (CFR). This figure is the accumulated value of capital expenditure which has yet to be expensed or paid for through revenue or capital resources. Each year the Council is required to apply revenue resources to reduce this outstanding balance (termed Minimum Revenue Provision).
- 4.5 Whilst the Council's CFR sets a limit on underlying need to borrow, the Council can manage the actual borrowing position by either;

- borrowing externally to the level of the CFR; or
- choosing to use temporary internal cash flow funds instead of borrowing; or
- a combination of the two.

- 4.6 The Council's CFR for the year was £112.762m as shown at Appendix A comprising:
- £76.751m relating to the core CFR,
 - £26.117m relating to business cases and
 - £9.894m relating to the Housing Revenue Account (HRA).

The actual CFR is lower than the approved estimate of £121.070m owing to rephasing of capital expenditure into 2022/23.

- 4.7 The Council's total long term external borrowing as at 31st March 2021 was £75.6m and increased to £90.655m at 31st March 2022. This increase reflects the proactive approach of managing interest rate risk, including securing borrowing of £17m to fund the Capital Investment plan, including borrowing for the Highlight, at a fixed interest rate of 2.31%. If we had delayed this decision we would have faced an annual budget pressures of £0.166m based on current PWLB rates.
- 4.8 The total borrowing remains below the CFR and there continued to be an element of netting down investments and borrowing. The Council needs to carefully manage the timing of new borrowing to fund forecast capital expenditure to secure affordable interest rates.

Prudential Indicators and Compliance Issues 2021/22

- 4.9 Details of each Prudential Indicator are shown at Appendix A. Some of the prudential indicators provide either an overview or specific limits on treasury activity. The key Prudential Indicators to report at outturn are described below.
- 4.10 The **Authorised Limit** is the "Affordable Borrowing Limit" required by Section 3 of the Local Government Act 2003. The Council does not have the power to borrow above this level. Appendix A demonstrates that during 2021/22 the Council has maintained gross borrowing within its Authorised Limit.
- 4.11 **Gross Borrowing and the CFR** - In order to ensure that borrowing levels are prudent, over the medium term the Council's external borrowing, must only be for a capital purpose. Gross borrowing should not exceed the CFR for 2021/22 plus the expected changes to the CFR over 2022/23 and 2023/24. The Council has complied with this Prudential Indicator.

The Treasury position 31st March 2022

- 4.12 The table below shows the treasury position for the Council as at the 31st March 2022 compared with the previous year:

Treasury position	31st March 2021		31st March 2022	
	Principal	Average Rate	Principal	Average Rate
Fixed Interest Rate Debt				
- PWLB	£30.6m	3.32%	£28.5m	3.40%
- Market Loans (Annuity)	-	-	£16.9m	2.31%
- Market Loans (Maturities)	£25.0m	3.92%	£25.0m	3.92%
- Non Market Loans (Maturities)	-	-	£0.3m	0.00%
- Market Loans (LOBOs)	£20.0m	4.12%	£20.0m	4.12%
Total Long Term Debt	£75.6m	3.73%	£90.7m	3.49%
Total Investments	£20.5m	0.05%	£45.8m	0.19%
Net borrowing Position	£55.1m		£44.9m	

- 4.13 At the time the LOBOs were taken out the prevailing PWLB rates were between 4.25% and 4.55%. The LOBOs have therefore allowed the Council to achieve annual interest savings between 0.13% and 0.43% compared to prevailing PWLB loans.
- 4.14 A key performance indicator shown in the above table is the very low average rate of external debt of 3.49% for debt held as at 31st March 2022. This is a historically low rate for long term debt and the resulting interest savings have already been built into the Medium Term Financial Strategy.
- 4.15 The Council's investment policy is governed by the Department for Levelling Up, Housing and Communities (DLUHC) guidance, which has been implemented in the annual investment strategy approved by Council.
- 4.16 The Council does not rely solely on credit ratings and takes a more pragmatic and broad based view of the factors that impact on counterparty risk. As part of the approach to maximising investment security the Council has also kept investment periods short (i.e. in most cases between three and six months but a maximum of one year). The downside of this prudent approach is that the Council achieved slightly lower investment returns than would have been possible if investments were placed with organisations with a lesser financial standing and for longer investment periods. However, during 2021/22 the risk associated with these higher returns would not have been prudent.
- 4.17 A prudent approach will continue to be adopted in order to safeguard the Council's resources.

Regulatory Framework, Risk and Performance 2021/22

- 4.18 The Council's treasury management activities are regulated by a variety of professional codes, statutes and guidance:

- The Local Government Act 2003 (the Act), which provides the powers to borrow and invest as well as providing controls and limits on this activity;
- The Act permits the Secretary of State to set limits either on the Council or nationally on all local authorities restricting the amount of borrowing which may be undertaken (although no restrictions have been made since this power was introduced);
- Statutory Instrument (SI) 3146 2003, as amended, develops the controls and powers within the Act, and requires the Council to undertake any borrowing activity with regard to the CIPFA Prudential Code for Capital Finance in Local Authorities;
- The SI also requires the Council to operate the overall treasury function with regard to the CIPFA Code of Practice for Treasury Management in the Public Services;
- Under the Act the DLUHC has issued Investment Guidance to structure and regulate the Council's investment activities;
- Under section 238(2) of the Local Government and Public Involvement in Health Act 2007 the Secretary of State has taken powers to issue guidance on accounting practices. Guidance on Minimum Revenue Provision was issued under this section on 8th November 2007.

4.19 The Council has complied with all of the above relevant statutory and regulatory requirements which limit the levels of risk associated with its Treasury Management activities

5. TREASURY MANAGEMENT STRATEGY 2022/23 1st QUARTER REVIEW

5.1 The Treasury Management Strategy for 2022/23 was approved by Council on 24th February 2022. The Council's borrowing and investment position as at 30th June 2023 is summarised as follows:

	£m	Average Rate
PWLB Loans	28.4	3.41%
Market Loan (Annuity)	17.0	2.31%
Market Loans (Maturities)	25.0	3.92%
Non-Market Loans (Maturities)	0.3	0.00%
Market Loans (LOBOs)	20.0	4.12%
Gross Debt	90.5	3.49%
Investments	46.5	0.50%
Net Debt as at 30-09-21	44.0	

5.2 Net Debt has decreased since 31st March 2022 owing to positive cash flows. It is anticipated that the net debt will increase towards the end of the year as this funding is expended and the capital programme progresses.

5.3 As part of the Treasury Strategy for 2022/23 the Council set a number of prudential indicators. Compliance against these indicators is monitored on a regular basis and there are no breaches to report.

6.1 CIPFA Treasury Management Code of Practice

- 6.2 The Council has adopted the current CIPFA Treasury Management Code of Practice, effective from December 2021.
- 6.3 Full adoption is not required until 1st April 2023, however they are encouraging Local Authorities to early adopt elements of the new code.

Treasury Management Advisors

- 6.4 The Council uses Link Asset Services – Treasury as its external treasury management advisors.
- 6.5 The Council recognises that responsibility for treasury management decisions remains with the organisation at all times and will ensure that undue reliance is not placed upon our external service providers.
- 6.6 It also recognises that there is value in employing external providers of treasury management services in order to acquire access to specialist skills and resources. The Council will ensure that the terms of their appointment and the methods by which their value will be assessed are properly agreed and documented, and subjected to regular review.

7. RISK IMPLICATIONS

- 7.1 There is a risk in relation to the level of interest rates the Council is able to secure for long term borrowing and the proposals detailed in this report are designed to manage these risks.
- 7.2 There are also risk implication in relation to the investment of surplus cash and these are addressed in the strategy recommended in the Counterparty limits.

8. FINANCIAL CONSIDERATIONS

- 8.1 As detailed in preceding paragraphs

9. LEGAL CONSIDERATIONS

- 9.1 The report details how the Council will comply with the relevant legal and regulatory requirements in relation to Treasury Management activities.

10. OTHER CONSIDERATIONS

Child and Family Poverty considerations	No relevant issues
Equality and Diversity considerations	No relevant issues
Staff Considerations	No relevant issues
Asset Management considerations	No relevant issues
Environment, sustainability and climate change considerations	No relevant issues

11. RECOMMENDATIONS

11.1 It is recommended that Members note the following:

- i) Note the 2021/22 Treasury Management Outturn detailed in section 4 and Appendix A.
- ii) Note the 2022/23 Treasury Management 1st Quarter Position detailed in section 5.

12. REASON FOR RECOMMENDATIONS

12.1 To allow Members to fulfil their responsibility for scrutinising the Treasury Management Strategy

13. BACKGROUND PAPERS

Treasury Management Strategy, report to Audit and Governance Committee 10th February 2022.

14. CONTACT OFFICER

Chris Little
Director of Resources and Development
Chris.Little@hartlepool.gov.uk
01429 523003

Appendix A

Prudential Indicators 2021/22 Outturn1. Ratio of Financing Costs to Net Revenue Stream

This indicator shows the proportion of the total annual revenue budget that is funded by the local tax payer and Central Government, which is spent on servicing debt.

2021/22 Estimate		2021/22 Outturn
4.77%	Ratio of Financing costs to net revenue stream	3.74%

2. Capital Expenditure

This indicator shows the total capital expenditure for the year.

2021/22 Estimate £'000		2021/22 Outturn £'000
31,282	Capital Expenditure	18,555

The actual is lower than estimated owing to the phasing of capital expenditure between years.

3. Capital Expenditure Financed from Borrowing

This shows the borrowing required to finance the capital expenditure programme, split between core expenditure and expenditure in relation to business cases.

2021/22 Estimate £'000		2021/22 Outturn £'000
175	Core Capital Expenditure Financed by Borrowing	2,437
7,153	Business Case Capital Expenditure Financed by Borrowing	4,974
2,349	HRA Capital Expenditure Financed by Borrowing	-
9,677	Total Capital Expenditure Financed by Borrowing	7,411

The actual is lower than estimated owing to the delay in supply of DSO Vehicle Procurement and the delay of HRA Capital Expenditure financed by Borrowing.

4. Capital Financing Requirement

CFR is used to determine the minimum annual revenue charge for capital expenditure repayments (net of interest). It is calculated from the Council's Balance Sheet and is shown below. Forecasts for future years are directly influenced by the capital expenditure decisions taken and the actual amount of revenue that is set aside to repay debt.

2021/22 Estimate £'000		2021/22 Outturn £'000
75,398	Core Capital Financing Requirement	76,751
33,509	Business Case Capital Financing Requirement	26,117
12,163	HRA Capital Financing Requirement	9,894
121,070	Total Capital Financing Requirement	112,762

The capital financing requirement is lower than estimated owing to the phasing of capital expenditure.

5. Authorised Limit for External Debt

The authorised limit determines the maximum amount the Council may borrow at any one time. The authorised limit covers both long term borrowing for capital purposes and borrowing for short term cash flow requirements. The authorised limit is set above the operational boundary to provide sufficient headroom for operational management and unusual cash movements. In line with the Prudential Code, the level has been set to give the Council flexibility to borrow up to three years in advance of need if more favourable interest rates can be obtained.

2021/22 Limit £'000		2021/22 Peak £'000
155,000	Authorised limit for external debt	92,250

The above Authorised Limit was not exceeded during the year. The level of debt as at 31st March 2022, excluding accrued interest was £90.655m. The peak level during the year was £92.250m.

6. Operational Boundary for External Debt

The operational boundary is the most likely prudent, but not worst case scenario, level of borrowing without the additional headroom included within

the authorised limit. The level is set so that any sustained breaches serve as an early warning that the Council is in danger of overspending or failing to achieve income targets and gives sufficient time to take appropriate corrective action.

2021/22 Limit £'000		2021/22 Peak £'000
145,000	Operational boundary for external debt	92,250

The operational limit was not exceeded in the year. The peak level of debt was £92.250m.

7. Interest Rate Exposures

This indicator is designed to reflect the risk associated with both fixed and variable rates of interest, but must be flexible enough to allow the Council to make best use of any borrowing opportunities.

2021/22 Limit %	Upper limits on fixed and variable interest rate exposure	2021/22 Peak %
100% 75%	Fixed Rates Variable Rates	77% 22%

The figures represent the peak values during the period.

8. Maturity Structure of Borrowing

This indicator is designed to reflect and minimise the situation whereby the Council has a large repayment of debt needing to be replaced at a time of uncertainty over interest rates, but as with the indicator above, it must also be flexible enough to allow the Council to take advantage of any borrowing opportunities.

	Upper Limit	Lower Limit	Actual by Maturity Date	Actual by soonest call date
	£000	£000	£000	£000
Less than one year	131,000	0	788	5,788
Between one and five years	141,000	0	3,420	18,420
Between five and ten years	141,000	0	4,469	4,469
Between ten and fifteen years	141,000	0	3,509	3,509
Between fifteen and twenty years	141,000	0	2,214	2,214
Between twenty and twenty-five years	141,000	0	2,391	2,391
Between twenty-five and thirty years	141,000	0	3,132	3,132
Between thirty and thirty-five years	141,000	0	6,336	6,336
Between thirty-five and forty years	141,000	0	19,050	19,050
Between forty and forty-five years	141,000	0	268	268
More than forty-five years	141,000	0	45,076	25,076

9. Investments Maturing over One Year

This sets an upper limit for amounts invested for periods longer than 364 days. The limit was not exceeded as a prudent approach to investment has been taken owing to uncertainties in the economy this is in line with the Treasury Management Strategy. Consequently all investments made during the year were limited to less than one year.

	1 year £000	2 year £000	3 year £000
Maximum Limit	20,000	0	0
Actual	0	0	0

AUDIT AND GOVERNANCE COMMITTEE

29th September 2022



Report of: Head of Audit and Governance

Subject: INTERNAL AUDIT PLAN 2022/23 UPDATE

1. PURPOSE OF REPORT

- 1.1 To inform Members of the progress made to date completing the internal audit plan for 2022/23.

2. BACKGROUND

- 2.1 In order to ensure that the Audit and Governance Committee meets its remit, it is important that it is kept up to date with the ongoing progress of the Internal Audit section in completing its plan. Regular updates allow the Committee to form an opinion on the controls in operation within the Council. This in turn allows the Committee to fully review the Annual Governance Statement, which will be presented at this meeting of the Committee, and after review, will form part of the statement of accounts of the Council.

3. PROPOSALS

- 3.1 That members consider the issues within the report in relation to their role in respect of the Councils governance arrangements. In terms of reporting internally at HBC, Internal Audit produces a draft report which includes a list of risks currently faced by the client in the area audited. It is the responsibility of the client to complete an action plan that details the actions proposed to mitigate those risks identified. Once the action plan has been provided to Internal Audit, it is the responsibility of the client to provide Internal Audit with evidence that any action has been implemented by an agreed date. The level of outstanding risk in each area audited is then reported to the Audit and Governance Committee.
- 3.2 The benefits of this reporting arrangement are that ownership of both the internal audit report and any resulting actions lie with the client. This reflects the fact that it is the responsibility of management to ensure adequate procedures are in place to manage risk within their areas of operation, making managers more risk aware in the performance of their duties. Greater assurance is gained that actions necessary to mitigate risk are implemented and less time is spent by both Internal Audit and management in ensuring audit reports are agreed. A greater breadth of assurance is given

to management with the same Internal Audit resource and the approach to risk assessment mirrors the corporate approach to risk classification as recorded in covalent. Internal Audit can also demonstrate the benefit of the work it carries out in terms of the reduction of the risk faced by the Council.

- 3.3 Table 1 summarises the assurance placed on those audits completed with more detail regarding each audit and the risks identified and action plans agreed provided in Appendix A.

Table 1

Audit	Assurance Level
Highways Repairs	Satisfactory
Cash/Bank	Satisfactory
Covid Outbreak Management Fund Grant	Satisfactory
Council Tax	Satisfactory
Non Domestic Rates	Satisfactory
Software Controls	Satisfactory
Universal Drug Treatment Grant	Satisfactory
Iclipse Controls	Satisfactory
IWorld Controls	Satisfactory
Integra Controls	Satisfactory
Controcc/Carefirst Controls	Satisfactory
Officers Expenses	Satisfactory
Treasury Management	Satisfactory
Youth Employment Initiative Q4	Satisfactory
VAT	Satisfactory
Covid Bus Service Support Grant	Satisfactory
Health and Safety	Satisfactory
Social Care Financial Assessments	Satisfactory

- 3.4 For Members information, Table 2 below defines what the levels of assurance Internal Audit places on the audits they complete and what they mean in practice:

Table 2

Assurance Level	Meaning
Satisfactory Assurance	Controls are operating satisfactorily and risk is adequately mitigated.
Limited Assurance	A number of key controls are not operating as intended and need immediate action.
No Assurance	A complete breakdown in control has occurred needing immediate action.

- 3.5 As well as completing the audits previously mentioned, Internal Audit staff have been involved with the following working groups:

- Information Governance Group.

- 3.6 Internal Audit staff are providing assurance to the Business, Energy and Industrial Strategy Department (BEIS) in respect of the payments of the Governments Business Support Grant Scheme and the Discretionary Business Support Grant Scheme. This requires us to provide detailed evidence supporting payments made to individuals and firms who were awarded those grants.
- 3.7 Table 3 below details the audits that were ongoing at the time of compiling the report.

Table 3

Audit	Objectives
Information Protection Policy	Ensure adequate policies/procedures are in place in line with statutory requirements.
Software Controls	Review the arrangements in place for managing software across the authorities IT infrastructure
Business Continuity/Disaster Recovery	An appropriately skilled and resourced emergency planning and continuity function is maintained which has developed a BC Policy and a BC Management System.
Risk Management	Ensure risk management strategies and policies are embedded across the organisation.
Leaving Care Allowances	Review eligibility to payments, carers payments are accurately and promptly processed and are in accordance with the Pathway Plan, care leavers payments are accurately and promptly processed and in accordance with the Pathway Plan, ensure a Pathway Plan is in place and this is regularly reviewed and ensure a Personal Advisor has been appointed.
Iclipse/Enterprise IT system	Ensure adequate IT controls are in operation.

4. RISK IMPLICATIONS

- 4.1 There is a risk that if Members of the Audit and Governance Committee do not receive the information needed to enable a full and comprehensive review of governance arrangements at the Council, this would lead to the Committee being unable to fulfil its remit.

5. FINANCIAL CONSIDERATIONS

- 5.1 There are no financial considerations.

6. LEGAL CONSIDERATIONS

- 6.1 There are no legal considerations.

7. CHILD AND FAMILY POVERTY CONSIDERATIONS

- 7.1 There are no child and family poverty considerations.

8. EQUALITY AND DIVERSITY CONSIDERATIONS

8.1 There are no equality and diversity considerations.

9. STAFF CONSIDERATIONS

9.1 There are no staff considerations.

10. ASSET MANAGEMENT CONSIDERATIONS

10.1 There are no asset management considerations.

11. ENVIRONMENT, SUSTAINABILITY AND CLIMATE CHANGE CONSIDERATIONS

11.1 There are no environment, sustainability and climate change considerations.

12. RECOMMENDATIONS

12.1 It is recommended that Members note the contents of the report.

13. REASON FOR RECOMMENDATIONS

13.1 To ensure that the Audit and Governance Committee meets its remit, it is important that it is kept up to date with the ongoing progress of the Internal Audit section in completing its plan.

14. BACKGROUND PAPERS

14.1 Internal Audit Reports.

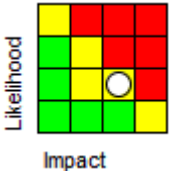
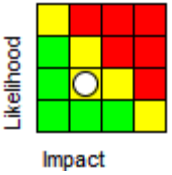
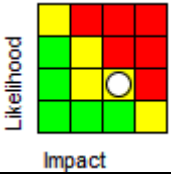
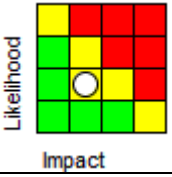
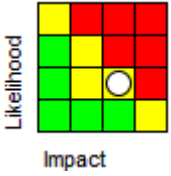
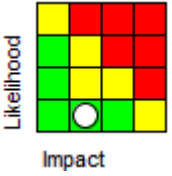
15. CONTACT OFFICER



15.1 Noel Adamson
Head of Audit and Governance
Civic Centre
Victoria Road
Hartlepool
TS24 8AY

Tel: 01429 523173

Email: noel.adamson@hartlepool.gov.uk

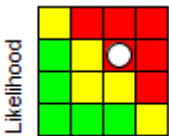



Appendix A

Audit	Objective	Assurance Level		
Highways Repairs and Maintenance	Effective budgetary control arrangements are in place; Work on the highways is procured in line with Contract procedure rules; Schemes are effectively managed to ensure that work is carried out to an appropriate standard, within budget and on time.	Satisfactory		
Risk Identified	Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented	
Highways defects may not be effectively rectified resulting in damage/injury to staff or members of the public. This may also lead to an insurance claim against the authority.		Highway Services have taken on 4 temporary staff, and have an advert out for 2 permanent staff.		
The Authority cannot give assurance that time and materials used was value for money.		This is works carried out by one section of the Council for another, and not involving a 3 rd party. There needs to be an element of trust that one section isn't over charging another, but none the less inspections of a small percentage of completed works are now being undertaken.		
The system may not be configured to the most recent version resulting in a loss of functionality or the system not being supported. Unauthorised/incorrect changes may be made to system parameters. Unauthorised access could be gained to the system resulting in inappropriate access to personal / sensitive information that may be used fraudulently or maliciously.		Currently awaiting CICT response on system upgrade to cloud provision.		

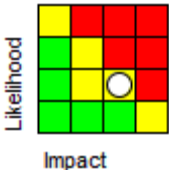
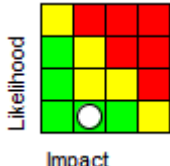
Unauthorised access could be gained to the system resulting in inappropriate access to personal / sensitive information that may be used fraudulently or maliciously.	 <p>Likelihood</p> <p>Impact</p>	Former employee's access rights have now been removed.	 <p>Likelihood</p> <p>Impact</p>
---	---	--	---

Audit	Objective			Assurance Level
Cash/Bank	Ensure clearly defined procedures are in place for the collection and banking of income and procedures for collecting income via the Internet & Cash Office are adequate and effective. All cash collections are promptly, completely and accurately recorded in the Authority's systems.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Contain Outbreak Management Fund	Ensure terms and conditions of grant adhered to.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Council Tax	Council Tax bills are issued in accordance with regulations and are accurate and complete; effective arrangements are in place to ensure all payments received in respect of Council Tax are identified promptly and accurately posted to individual accounts.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
Reputational damage to the Council if credit balances are not refunded to account holders.		 Likelihood Impact	Further resources to be utilised within the Revenues Team to reduce the number of refundable credits. This transfer of resource may impact on other areas within the team.	 Likelihood Impact
Discount may be awarded incorrectly resulting in incorrect liability		 Likelihood Impact	Move to a fully managed service with Datatank.	 Likelihood Impact



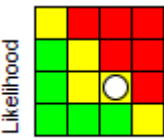
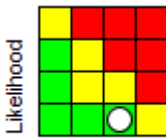
Audit	Objective			Assurance Level
Non Domestic Rates	Payments are received and processed accurately to bill payers' accounts.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

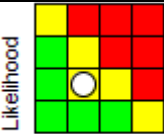
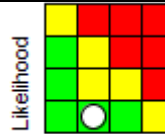

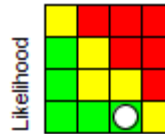

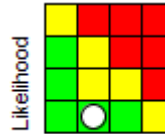
Audit	Objective			Assurance Level
Iclipse Software	Ensure adequate IT controls are in operation.			Satisfactory
Risk Identified	Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented	
Unauthorised access could be gained to the system resulting in inappropriate access to personal / sensitive information that may be used fraudulently or maliciously.		Decommission Iclipse solution when Enterprise issues are resolved. The implementation date is subject to satisfactory resolution of Enterprise Issues.		


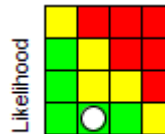
Audit	Objective			Assurance Level
IWorld Software	Ensure adequate IT controls are in operation.			Satisfactory
Risk Identified	Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented	
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Integra Software	Ensure adequate IT controls are in operation.			Satisfactory
Risk Identified	Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented	
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Resource Link Software	Ensure adequate IT controls are in operation.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Officers Expenses	Up to date Policy / procedures are in place that define procedures for processing and approving claims for reimbursement of employee expenses incurred. Arrangements in place ensure that claims are valid, accurate, and appropriately authorised and the scheme is operated in line with legislative requirements and other HBC policies.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
Claims may be overpaid if correct mileage is not claimed.		 Likelihood Impact	Communication to be issued to claimants and managers to remind them of the process and their responsibilities. We will issue after a review of procedures.	 Likelihood Impact
Claims and allowances may be paid without entitlement if appropriate arrangements for ensuring that claimants are appropriately qualified to complete journeys. Risk also exists that disqualified or uninsured drivers could be driving on Council business.		 Likelihood Impact	Review all outstanding licence and insurance documents to circulate to managers for review. This will include the instances where mileage has been claimed and this information is not held or up to date. Shared Services Manager to confirm with Assistant Director that information is appropriate to be issued.	 Likelihood Impact
Claims for reimbursement of expenditure incurred may not be valid if evidence of expenditure incurred is not provided with the			Communication to be issued to claimants and managers to remind them of the process and their responsibilities. We will issue after a review of procedures.	

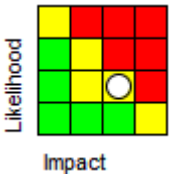
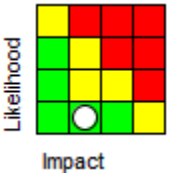
claim.			
Financial penalties may be incurred if VAT is not accounted for correctly.		Review of VAT transaction to be completed. Procedures to be reviewed and communication to be issued to claimants and managers of requirements.	
Staff may not be complying with corporate procedures if claims for reimbursement are not submitted on MyView / Resource link.		Review to be completed with Assistant Director to decide whether Cash Office and reimbursement of claims would be allowed in future.	

Audit	Objective			Assurance Level
Treasury Management	A Treasury Management Strategy is in place that complies with the Treasury Management in the Public Services: Code of Practice and Cross-Sectoral Guidance Notes (CIPFA, 2017) and Prudential Code for Capital Finance in Local Authorities (CIPFA, 2017) and where applicable the updated 2021 Code and Guidance.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
The use of external service providers may not represent value for money for the Authority.			Approval to extend the contract will be obtained via procurement.	

The Service may not comply with the requirements of the Anti-Money Laundering and Counter Terrorist Financing Policy.		To liaise with Assistant Director - Finance regarding the training available and who should receive this.	
---	--	---	--



Audit	Objective			Assurance Level
Youth Employment Initiative Q4	Ensure terms and conditions of grant adhered to.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective			Assurance Level
VAT	Review the arrangements in place for administering VAT to ensure that that staff involved in the processing of VAT are aware of their responsibilities, VAT categories are correctly identified, accounted for, and effective planning ensures efficient, effective and economic operations which maximise benefits to the Council.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
Arrangements for administering VAT procedures may not promote efficient and effective operations and maximise cash flow for the organisation.			Update VAT Manual	

Arrangements for administering VAT procedures may not promote efficient and effective operations and maximise cash flow for the organisation.		Perform partial exemption calculation using 2021/22 data.	
---	---	---	---

Audit	Objective			Assurance Level
Covid Bus Service Support Grant	Ensure terms and conditions of grant adhered to.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective			Assurance Level
Health and Safety Policy	Planned reviews and inspections are undertaken at appropriate intervals to determine whether suitable health and safety management arrangements are in place.			Satisfactory
Risk Identified		Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented
No unmitigated risk identified.				

Audit	Objective	Assurance Level		
Social Care Financial Assessments	Ensure robustness of the financial assessments process for determining services users' contribution	Satisfactory		
Risk Identified	Risk Level prior to action implemented	Action Agreed	Risk Level after action implemented	
Service users contributions may not be correctly calculated if financial assessments are not promptly & accurately processed in line with legislation / guidance.	 <p>Likelihood</p> <p>Impact</p>	Raise the issue highlighted in relation to Enterprise with Tim Rogers, who is responsible for Enterprise from a CICT perspective, and ask if there is anything that he can do/suggest to ensure the documents are available in full. I will include Trevor Smith, Head of Strategic Commissioning (Adults) in any emailed correspondence, as the senior manager responsible from a MIT perspective.	 <p>Likelihood</p> <p>Impact</p>	

AUDIT AND GOVERNANCE COMMITTEE

29 September 2022



Report of: Chief Solicitor

Subject: REGULATION OF INVESTIGATORY POWERS ACT
2000 (RIPA) ANNUAL REPORT (INCLUDING
QUARTER 1 UPDATE)

1. PURPOSE OF REPORT

- 1.1 To give an annual report to Elected Members on activities relating to surveillance by the Council and policies under the Regulation of Investigatory Powers Act 2010.

2. BACKGROUND RIPA

- 2.1 Hartlepool Borough Council has powers under the Regulation of Investigatory Powers Act 2000 (RIPA) to conduct authorised covert surveillance.
- 2.2 This report is submitted to members as a result of the requirement to report to Members under paragraph 4.47 of the Home Office Code of Practice for Covert Surveillance and Property Interference Revised (August 2018) which states that:

Elected members of a local authority should review the authority's use of the 1997 Act and the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 1997 Act and the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

3. BACKGROUND

- 3.1 All directed surveillances (covert, but not intrusive), use of covert human intelligence sources (CHIS) and acquisition of Communication's data require authorisation by a senior Council officer and the exercise of the powers is subject to review. The controls are in place in accordance with the Human Rights Act, particularly the right to respect for family and private life.

- 3.2 The Investigatory Powers Commissioner's Office (IPCO) now oversees the Council's exercise of surveillance powers under RIPA. This was formerly undertaken by the Office of Surveillance Commissioners (OSC).
- 3.3 A confidential database of authorised surveillances is maintained, charting relevant details, reviews and cancellations.
- 3.4 Substantial changes were made to the powers of Local Authorities to conduct directed surveillance and the use of human intelligence sources under the Protection of Freedoms Act 2012.
- 3.5 As from 1 November 2012 Local Authorities may only use their powers under the Regulation of Investigatory Powers Act 2000 to prevent or detect criminal offences punishable by a minimum term of 6 months in prison (or if related to underage sale of alcohol and tobacco. The amendment to the 2000 Act came into force on 1 November 2012.
- 3.6 Examples of where authorisations could be sought are serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The surveillance must also be necessary and proportionate. The 2012 changes mean that authorisations cannot be granted for directed surveillance for e.g. littering, dog control, fly posting.
- 3.7 As from 1 November 2012 any RIPA surveillance which the Council wishes to authorise must be approved by an authorising officer at the council and also be approved by a Magistrate; where a Local Authority wishes to seek to carry out a directed surveillance or make use of a human intelligence source the Council must apply to a single Justice of the Peace.
- 3.8 The Home Office have issued guidance to Local Authorities and to Magistrates on the approval process.

4. **RIPA AUTHORISATIONS**

- 4.1 In the period 2021/2022:-

Communications Data	0
CHIS	0
Directed Surveillance	1
Non-RIPA	1

- 4.2 In the quarter to the date of this meeting:

Communications Data	Nil
CHIS	Nil
Directed Surveillance	Nil
Non –RIPA	Nil

5. SURVEILLANCE POLICY

5.1 The Council's RIPA Policy is available on the Council's intranet and is appended to this report. A number of amendments were made to the Policy when last reviewed. Therefore, the only update is as follows:-

- Inconsistency in the policy removed to ensure that either Trading Standards officers or Legal Officer can make applications - consequently the flowchart on page 34 has been amended (Appendix 1) to read that a Local authority investigator *(or an appointed representative of the Legal Division)* to contact Her Majestys Court & Tribunals Service (HMCTS) court to arrange a hearing or the Local authority investigator *(and/or an appointed representative of the Legal Division)* attend court.

6. ACTIVITY IN THE CURRENT YEAR

6.1 The Authority's procedures continue to be reviewed in the light of changes in the law and guidance received including recent correspondence from the Investigatory Powers Commissioner's Office.

6.2 Discussions have taken place with the Principal Auditor. It has been agreed that rather than complete a full audit on HBC's RIPA policy there is scope to focus instead on asking questions as part of the audit planning process for each audit to determine if there are areas of the organisation where there might be investigatory work going on and also identify where that may utilise social media searches and verifying how they are doing this. A standard set of questions have been agreed as follows:-

1. Are there any instances where you or your team may undertake any type of investigatory work such as reviewing social media profiles of clients or service users?
2. If yes, have you received RIPA training?
3. If yes, have you considered the RIPA legislation and HBC's RIPA Policy to ensure your actions are legal, whether they need sign off via RIPA or non-RIPA procedures? Or have you sought guidance from Legal Services?
4. If yes, note what activities you undertake and how regularly these occur.

Feedback will be provided by the audit team where there is investigatory work happening in areas we may have been unaware of previously and an idea of how this is being done and whether it is in line with HBC's policy.

6.3 Training is continuing to be planned to take place annually, with the first sessions having taken place in 2019. Due to the restrictions of the Covid- 19 pandemic, training had to be suspended. However, so far this year, three members of the Trading Standards department have received RIPA training and the annual training regime has resumed for other staff members with

training scheduled to take place later this month on 22 September 2022 with Officers from a range of departments registered to attend.

- 6.4 Awareness of RIPA to continue to be raised across the Council.
- 6.5 Information continues to be made available on the RIPA pages of the Council's intranet and internet.

8. RECOMMENDATIONS

- 8.1 To review the Authority's use of the Regulation of Investigatory Powers Act 2000 and approve the updated RIPA policy.

9. REASONS FOR RECOMMENDATIONS

- 9.1 To enable the Council to operate the RIPA system effectively and as required by law and guidance.
- 9.2 Members of the Audit and Governance Committee are responsible for approving the RIPA Policy on an annual basis as referred to in Section 3 of the Policy.

10. CONTACT OFFICER

- 10.1 Hayley Martin
Chief Solicitor and Senior Responsible Officer for RIPA
Hayley.martin@hartlepool.gov.uk
01429 523003

11. BACKGROUND PAPERS

Home Office Code of Practice
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf



POLICY AND PROCEDURE

**ON THE USE OF COVERT SURVEILLANCE AND
ACQUISITION OF COMMUNICATION DATA**

**REGULATION OF INVESTIGATORY POWERS ACT 2000
AND INVESTIGATIVE POWERS ACT 2016**

Title	Regulation of Investigatory Powers Act 2000
Owner	Chief Solicitor
Version	5
Issue date	September 2022
Approved by	Chief Solicitor
Next Revision Due	September 2023

INDEX

1. Introduction
2. Background
3. Roles and Responsibilities
4. Local Authority Use of RIPA and the IPA
5. Types of Surveillance
6. Applications for Directed Surveillance and CHIS
7. Considering Applications for Directed Surveillance
8. Considering Applications for the use of CHIS
9. Applying for Judicial Approval
10. Acquisition and Disclosure of Communications Data
11. Authorisation for Acquisition of Communications Data
12. Working with other Agencies
13. Records Management

APPENDICES

- | | |
|------------|--|
| Appendix 1 | Judicial Approval Procedure |
| Appendix 2 | Procure for E-Crime, including Investigation of Social Networking Sites. |
| Appendix 3 | Non-RIPA Form |

1. **INTRODUCTION**

1.1 This document sets out the policy and procedures adopted by Hartlepool Borough Council (“the Council”) in relation to the use of Covert Surveillance Regulation of Investigatory Powers Act 2000 (“RIPA”) and Investigative Powers Act 2016 (IPA). Covert Surveillance includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications and it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. The documents also included the Council’s policy on the acquisition of communication data which includes service use information (such as the type of communication, the time of the communication or its duration, but not its content) and subscriber information (such as billing information).

1.2 For the purpose of this update, references to the Home Office Codes of Practice relate to:

- [Home Office Covert Human Intelligence Sources Code of Practice \(2018\)](#)
- [Home Office Covert Surveillance and Property Interference Revised Code of Practice \(2018\)](#)
- [Home Office Communications Data Code of Practice \(2018\)](#)

1.3 The following terms are used throughout this Policy:

RIPA	Regulation of Investigatory Powers Act 2000
IPA	Investigative Powers Act 2016
CHIS	Covert Human Intelligence Source
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
IPCO	Investigatory Powers Commissioners Office
NAFN	National Anti-Fraud Network
CSP	Communications Service Provider

1.4 It should be noted that any use of activities under RIPA or IPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary and proportionate to the matter being investigated.

1.5 Directed surveillance, use of a Covert Human Intelligence Source (CHIS) or acquisition of communications data by or on behalf of the Council must be

carried out in accordance with this Policy. Any such activity must be authorised by one of the Authorising Officers identified in Appendices 1 and 2. All authorisations must then be approved by a Magistrate before any covert activity takes place. Staff directly employed by the Council and any external agencies working for the Council are subject to RIPA whilst they are working in a relevant investigatory capacity.

- 1.6 The purpose of the Policy is to ensure the Council is acting lawfully while undertaking its various enforcement functions, ensuring directed surveillance, the use of a CHIS or acquisition of communication data is both necessary and proportionate, and takes into account the rights of individuals under Article 8 of the Human Rights Act,.

2. **BACKGROUND**

- 2.1 RIPA came into force on 25 September 2000 and was enacted in order to regulate the use of a range of investigative powers by a variety of public authorities. It gives a statutory framework for the authorisation and conduct of certain types of covert surveillance operations. The aim of the legislation is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action.
- 2.2 It is consistent with the Human Rights Act 1998 and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (right to respect for a person's private and family life, home and correspondence). Compliance with RIPA means that any conduct authorised under it is "lawful for all purposes". This important protection derives from Section 27(1) of RIPA, which gives the authorised person an entitlement to engage in the conduct which has been authorised. Compliance with RIPA will assist the Council in any challenges to the way in which evidence has been gathered and will enable the Council to demonstrate that it has acted lawfully.
- 2.3 The single ground for a Council's application for a surveillance authorisation is 'Preventing or detecting crime or disorder'. Since the making of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2012, the Council can only grant an authorisation for the use of directed surveillance where the offence being investigated attracts a custodial sentence of six months or more or when investigating a criminal offence relating to the underage sale of alcohol or tobacco.
- 2.4 Part 3 of the Investigatory Powers Act 2016 ('IPA) permits certain public bodies to acquire specified types of communications data in limited circumstances, subject to prior authorisation granted in accordance with the

IPA. Part 3 applies principally to the police and central government departments and agencies, including defence, security and intelligence bodies. The power it grants to local authorities is less extensive, limiting the acquisition of data to cases involving the prevention or detection of serious crime.

- 2.5 The communications data which, in defined circumstances, local authorities are permitted to obtain under the Act is known as 'entity data' and 'events data'. In brief, data of this nature can identify who a suspected offender has been in communication with via their telephone or e-mail, as well as where that communication was made or received.
- 2.6 This policy addresses solely issues having relevance to the activities of Hartlepool Borough Council.
- 2.7 Compliance with RIPA makes authorised surveillance "lawful for all purposes" pursuant to Section 27(1) of the Act. Compliance with RIPA will protect the Council from challenges to both the gathering of, and the subsequent use of, covertly obtained information. Non-compliance with RIPA legislation may result in:
- (a) evidence being found inadmissible by the Courts;
 - (b) a complaint of maladministration to the Ombudsman; or
 - (c) A complaint to the Investigate Power Tribunal who can order compensation be paid to the individual.
- 2.8 It is therefore essential that the Council's policies and procedures, as set out in this document, are followed.

3. ROLES AND RESPONSIBILITIES

3.1 Senior Responsible Officer (SRO):

- 3.1.1 The role of SRO will be undertaken by the Council's Chief Solicitor
- 3.1.2 In accordance with good practice the SRO will be responsible for:
- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;
 - Compliance with Part 2 of the Act and with the Home Office Codes of Practice;
 - Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the

implementation of processes to minimise repetition of errors;

- Engagement with the Investigatory Powers Commissioner's Office (IPCO) when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.
- Produce a report to the Council's Audit and Governance Committee on the Council's use of RIPA

3.2 Authorising Officers

- 3.2.1 For RIPA Applications (Directed Surveillance & use of a CHIS) the Authorising Officers is an officer of the Council, who can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by Officers. Authorising Officers may not sub-delegate their powers in relation to RIPA to other Officers.
- 3.2.2 The Officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.
- 3.2.3 For the purpose for standard authorisations (where it is not likely that confidential information will be acquired)
- Head of Paid Service
 - Director of Regeneration and Neighbourhood Services
 - Senior Responsible Officer (in the absence of the above)
- 3.2.4 For authorizations where it is likely that confidential information will be acquired or where using a CHIS who is a juvenile (under 18, JCHIS) or a vulnerable individual
- Head of Paid Service
 - Senior Responsible Officer (exceptional circumstances)
- 3.2.5 In relation to communications data the authorising individual is Office for communications Data Authorisations ('OCDA') who act on behalf of the Investigatory Powers Commissioner.
- ### 3.3 RIPA Co-ordinator:
- 3.3.1 The Legal and Democratic Services Team Manager is appointed RIPA Co- coordinator.
- 3.3.2 The RIPA Co-ordinator shall:-
- have overall responsibility for the management and oversight of requests

and authorisations under RIPA;

- issue a unique reference number to each authorisation requested under RIPA (this must be before the application has been authorised);
- retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer, maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;
- review and monitor all forms and documents received to ensure compliance with the relevant law and guidance and this policy and procedures document and informing the Authorising Officer of any concerns;
- chase failures to submit documents and/or carry out reviews/ cancellations;
- be responsible for organising a corporate RIPA and IPA training programme;
- ensure corporate awareness of RIPA and IPA; its value as a protection to the Council is maintained;

3.4 Elected Members:

3.4.1 Members of the Council's Audit and Governance Committee will approve the RIPA policy on an annual basis.

3.4.2 Members of the Council's Audit and Governance Committee will receive the following information on a quarterly basis:

Information to be provided	Frequency
The number of RIPA authorisations requested and granted	Quarterly report Annual Report
The number of joint operations where RIPA authorisation has been	Quarterly Report Annual report
Review of the effectiveness of this policy and any recommendation for	Annual Report – with any significant

3.4.3 Elected Members will have no involvement in making decisions as to

whether authorisations are approved.

4. LOCAL AUTHORITY USE OF RIPA AND THE IPA

- 4.1 RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by Council Officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.
- 4.2 RIPA limits local authorities to using three covert techniques, as set out below:
 - a) Directed surveillance is essentially covert surveillance in places other than residential premises or private vehicles
 - b) A Covert Human Intelligence Source (CHIS) includes undercover Officers, public informants and people who make test purchases (for enforcement purposes)
- 4.3 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data: service use and subscriber information. Under no circumstances can local authorities be authorised to obtain traffic data under RIPA.
- 4.4 Directed surveillance may only be authorised under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.
- 4.5 Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Requests for authorisation must still demonstrate how the activity is both proportionate and necessary.
- 4.6 A local authority may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and flyposting.
- 4.7 Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more include more serious criminal damage and dangerous waste dumping
- 4.8 Directed surveillance will always be a last resort in an investigation, and use

of a CHIS by the Council is unlikely. These activities will only be undertaken where there is no other reasonable and less intrusive means of obtaining the information.

- 4.9 In cases of joint working with other agencies, for example the Department for Work and Pensions or the Police, only one authorisation from one organisation is required. This should be made by the lead authority for the particular investigation. Council Officers should satisfy themselves that authorisation has been obtained and be clear exactly what activity has been authorised. All cases of overt or covert surveillance undertaken in joint working with other authorities or organisations will be reported to the Audit and Governance Committee in accordance with paragraph 3.6.2 above
- 4.10 The IPA allows the Council to gain authorisation for access to communication data, including 'entity data' and 'events data' and includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written. This Authorisation must be granted by the Investigative Powers Commissioner.
- 4.11 A Single Point of Contact (SPoC) is required to undertake the practical facilitation with the communications service provider (CSP) in order to obtain the data requested. The SPoC must have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the local authority and CSP.
- 4.12 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities. Compliance with the provisions of RIPA, the Home Office Codes of Practice and this policy and procedures should protect the Council, its Officers and agencies working on its behalf against legal challenge. Section 27 of RIPA states that "conduct...shall be lawful for all purposes if an authorisation...confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation". If correct procedures are not followed, the Council could be rendered liable to claims and the use of the information obtained may be disallowed in any subsequent legal proceedings.

5. TYPES OF SURVEILLANCE

- 5.1 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA and the IPA. In many cases investigations carried out by Council Officers will not be subject to RIPA or the IPA, as they involve overt rather than covert surveillance (see below). An explanation of terms used is set out below:
- 5.2 'Surveillance' includes
 - monitoring, observing, listening to persons, watching or following

their movements, listening to their conversations and other such activities or communications;

- recording anything mentioned above in the course of authorised surveillance;
- Surveillance by, or with the assistance of, appropriate surveillance

device(s). Surveillance can be overt or covert.

5.2.1 Covert Surveillance

- Covert surveillance is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place.
- RIPA requires the authorisation of two types of covert surveillance (directed surveillance and intrusive surveillance) plus the use of covert human intelligence sources (CHIS) or acquisition of communications data.

5.3 Directed Surveillance

5.3.1 Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance ;
- it is conducted for the purposes of a specific investigation or operation;
- it 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);
- 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 under Part II of the 2000 Act to be sought.

5.3.2 Such forms of surveillance involve observing an individual or group of people whether through unaided observation or listening or through the use of technical devices and when information regarding their private or family lives is likely to be obtained.

Example: Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.

5.3.3 Special provisions apply where information enjoying legal privilege or certain types of confidentiality may be obtained. In such circumstances, which are not expected to be relevant to the Council's activities, the approval of the **Council's Head of Paid Service** is required, or in his/her absence by the Council's Chief Solicitor.

5.4 Covert Human Intelligence Sources (CHIS)

5.4.1 Under the RIPA, a person is a CHIS if:

- they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 26(8)(b) or (c);
- they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

5.4.2 A person may be a CHIS if they induce, ask or assist another person to engage in the conduct described above.

5.4.3 Carrying out test purchases will not require the purchaser to establish a relationship with the supplier for the purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS, for example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter) although an Officer covertly watching a particular transaction may require an authorisation for directed surveillance.

5.4.4 By contrast, developing a relationship with a person in the shop, for example to obtain information about the seller's supplier of an illegal or unsafe product, will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is happening in the shop will require authorisation as directed surveillance. A combined authorisation can be given for CHIS and also directed surveillance.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary.

However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

5.5 Acquisition and Disclosure of Communications data

- 5.5.1 Within this policy, the term ‘communications data’ means ‘entity data’ and ‘events data’ and includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content i.e. what was said or written.
- 5.5.2 A Council cannot make an application that requires the processing or disclosure of internet connection records for any purpose.
- 5.5.3 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services. All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories of entity data and events data.
- 5.5.4 **Entity data** means any data which—
- 5.5.5 (a) is about—
- (i) an entity (a person or thing such as a phone, tablet or computer),
 - (ii) an association between a telecommunications service and an entity, or
 - (iii) an association between any part of a telecommunication system and an entity,
- (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and
- (c) is not events data.
- 5.5.6 Entity data covers information about a person or thing, and about links between a telecommunications system and a person or thing that

identifies or describes the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

5.5.7 Examples of entity data include:

- Subscriber checks such as “who is the subscriber of phone number 01234 567 890?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space www.example.co.uk?”
- subscribers’ or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and information about selection of preferential numbers or discount calls.

5.5.8 **Events Data** is more intrusive and means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

5.5.9 Events data includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication

5.5.10 Events data can also include the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications.

5.5.11 Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed)
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Obtaining Communications Data

- 5.5.12 Part 3 of IPA contains provisions relating to authorisations for obtaining communications data.
- 5.5.13 This part of IPA is now in force but the acquisition of communications data was previously covered by RIPA. Under RIPA, local authorities were required to obtain judicial approval in order to acquire communications data. However, the position has now changed and from June 2019, all communications data applications must instead be authorised by the Office for Communications Data Authorisations (“the OCDA”).
- 5.5.14 The Home Office issued ‘Communications Data’ Code of Practice in November 2018 and chapter 8 covers local authority procedures. A local authority must make a request to obtain communications data via a single point of contact (“SPoC”) at the National Anti-Fraud Network (“NAFN”). In addition to being considered by a NAFN SPoC, an officer within the local authority of the rank of service manager or above should be aware the application is being made before it is submitted to an authorising officer in the OCDA.
- 5.5.15 A serious crime threshold applies to the obtaining of some communications data. The council can only submit an application to obtain events data for the investigation of a criminal offence capable of attracting a sentence of 12 months or more. However, where the council is looking to obtain entity data this can be done for any criminal investigation where it is necessary and proportionate to do so.

5.6 Overt Surveillance

- 5.6.1 Overt Surveillance will include most of the surveillance carried out by the Council, there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV cameras normally amount to overt surveillance. In many cases, Officers will be going about Council business openly (e.g. a parking attendant patrolling a Council car park).
- 5.6.2 However, care must be taken to ensure that Officers are not intentionally acting as members of the public in order to disguise their true intent as this may then be considered as covert and require RIPA authorisation.
- 5.6.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that Officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.
- 5.6.4 Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer
- 5.6.5 Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by Enforcement Officers as part of general observation does not need to be regulated by RIPA, as long as the systematic surveillance of an individual is not involved. However, if binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. Any such surveillance will be intrusive “if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle”. The quality of the image obtained rather than the duration of the observation is what is determinative. It should be remembered that the Council is not permitted to undertake intrusive surveillance.
- 5.6.6 Similarly, although signposted, CCTV cameras do not normally require

authorisation, this will be required if the camera(s) are to be directed for a specific purpose which involves prolonged surveillance on a particular person.

5.6.7 Use of body worn cameras should be overt. Badges should be worn by Officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

5.6.8 Surveillance that is unforeseen and undertaken as an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation normally falls outside the definition of directed surveillance and therefore authorisation is not required. However, if a specific investigation or operation is subsequently to follow, authorisation must be obtained in the usual way before it can commence. In no circumstances will any covert surveillance operation be given backdated authorisation after it has commenced.

5.7 Social Networking Sites (SNS)

5.7.1 The revised Code of Practice Covert Surveillance and Property Interference Revised Code of Practice states that:

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

The internet may be used for intelligence gathering and/or as a surveillance tool. 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, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if

no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

set out in paragraph 3.14 below, 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. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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. 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.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

Example 1: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be

sought.)

Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 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. However, 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.

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- 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 (taking account of the guidance at paragraph 3.6 above);*
- 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.*

Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it

would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

5.7.2 The Council's Policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below as well as in the attached procedure note at Appendix 2:

- Officers must not 'friend' individuals on social networks;
- Officers must not use their own private accounts to view the social networking accounts of other individuals;
- Officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation. Such viewing can take a backward look at the individual's profile;
- further viewing of open profiles on social networking sites to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate. However, if the activity being investigated does not fall within the protection of RIPA, for example, if the crime threshold is not met, then a non-RIPA form must be completed and authorised (Appendix 3);
- Officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

5.8 Intrusive Surveillance

5.8.1 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.

5.8.3 Intrusive surveillance cannot be carried out or approved by the Council. Only the police or other law enforcement agencies are permitted to use such powers.

5.8.4 The Council recognises that forms of notice requiring the provision of communications data are subject to inspection by IPCO and both applicant and Designated Officer may be required to justify their decisions.

6. APPLICATIONS FOR AUTHORISATIONS OF DIRECTED SURVEILLANCE AND CHIS

6.1 Before commencing any investigatory action which is to involve:

- covert directed surveillance; or
- the use or conduct of a Covert Human Intelligence Source.

6.2 The Officer responsible for the investigation shall submit the relevant form of application for authorisation to the appropriate Authorising Officer. The investigatory action shall not be commenced unless and until the Authorising Officer has granted the application as signified by the Authorising Officer endorsing the application with his/her approval and returning one copy to the applicant.

6.3 Forms are available from the Home Office website at the link below
<https://www.gov.uk/government/collections/ripa-forms--2>

6.4 The application form shall be submitted not less than 7 days before the intended date of commencement of the investigatory action.

6.5 All information required in the application form shall be provided. In particular the description of the activity proposed shall be sufficient to enable the Authorising Officer to judge whether the authorisation applied for is **necessary and proportionate** (see below).

6.6 Review

6.6.1 Each Authorising Officer shall determine the standard review period for authorisations granted by him/her and should be at least monthly. More frequent review periods may apply to authorisations for different categories of investigatory action where circumstances demand. Not later than 3 working days before the expiration of the review period for an authorisation relating to an ongoing investigation, the Officer responsible for the investigatory action shall submit a Review of Authorisation form to the Authorising Officer who granted the authorisation. Unless the circumstances warrant the continuation of an authorisation, it should be cancelled.

6.7 Renewal

- 6.7.1 An Investigating Officer who has received an authorisation is responsible for renewing that authorisation if the activity for which authorisation was given is expected to continue beyond the duration of the authorisation. Renewal applications should be made before the initial authorisation expires on the appropriate form.
- 6.7.2 An application for renewal must be made to the Authorising Officer who granted the initial authorisation.

6.8 Cancellation

- 6.8.1 The investigating officer responsible for undertaking the authorised surveillance must apply to have that authorisation cancelled when the investigation or operation for which authorisation was given has ended, the authorised surveillance activity has been completed, or the information sought is no longer necessary.

6.9 Expiration and Review of Authorisations

- 6.9.1 Unless renewed or cancelled the maximum duration of a:
- Directed Surveillance - 3 months from the date of Magistrate's approval of an authorisation or renewal of authorisation in each case;
 - Covert Human Intelligence Source authorisation - 12 months (or 1 month if the CHIS is under 18) from the date of Magistrate's approval
- 6.9.2 No authorisation can be left to expire, and should always be cancelled using the relevant form.

7. **CONSIDERING APPLICATIONS FOR DIRECTED SURVEILLANCE**

Step 1: Is authorisation needed for this activity?

- 7.1 An Authorising Officer must first consider whether the proposed surveillance is to cover activity which:
- Amounts to a criminal offence which attracts a term of 6 months imprisonment; or
 - Is related to the underage sale of alcohol and tobacco.

- 7.2 To require authorisation, the activity to which the application relates must be covert and must involve the obtaining of private information on an individual through directed surveillance.
- 7.3 An Authorising Officer should interpret the definitions broadly when determining whether an activity is covert or if private information will be obtained. When in doubt, the authorisation procedure must always be followed.
- 7.4 At no time can an Authorising Officer authorise any intrusive surveillance.

Step 2: Is the activity necessary?

- 7.5 An Authorising Officer can only authorise an activity where s/he believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing or detecting crime or of preventing disorder.
- 7.6 The Authorising Officer must be satisfied that there are no other reasonable means of carrying out the investigation, or obtaining the desired information, without undertaking the activity for which authorisation is sought.
- 7.7 Authorisation should not be granted if the information sought can be obtained by other means without undertaking an activity which falls under the requirements of RIPA. Authorisation cannot be granted if it is for any purpose other than the prevention or detection of crime or for the prevention of disorder.

Step 3: Is it proportionate?

- 7.8 If the activity is necessary, the Authorising Officer must also believe that the activity is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the activity against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the particular circumstances or if the information sought could reasonably be obtained by less intrusive means. Any activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair.
- 7.9 An Authorising Officer should first consider the following primary factors in determining whether the activity for which authorisation is sought is proportionate:

Confidential Information

- 7.10 The Authorising Officer must take into account the likelihood of confidential information being acquired. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.
- 7.11 Where confidential information is likely to be acquired, authorisation should

only be given in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

- 7.12 In these circumstances, the Authorising Officer must be the Head of Paid Service or Senior Responsible Officer (exceptional circumstances),

Risk of Collateral Intrusion

- 7.13 The Authorising Officer must consider whether there is a risk of collateral intrusion into the private life of any person not the primary subject of the investigation. The applicant should describe the activity sufficiently widely to include not only named individuals but also any others who may be at risk of collateral intrusion to enable this consideration to occur.
- 7.14 Where the risk of such intrusion is sufficiently significant, the Authorising Officer must determine whether a separate authorisation is required in respect of these other persons.
- 7.15 The person carrying out the activity must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation needs to be amended and re-authorised or a new authorisation is required.
- 7.16 The following further considerations must then be considered in determining whether the activity for which authorisation is sought is proportionate:
- The reasons given by the applicant as to why that activity is sufficient and adequate for obtaining the information sought;
 - Whether there are any other reasonable means of obtaining the information sought;
 - Whether the surveillance is an essential part of the investigation;
 - The type and quality of the information the activity will produce and its likely value to the investigation;
 - The amount of intrusion, other than collateral intrusion, the activity will cause and whether there are ways to minimise that intrusion; and
 - The length of time for which the authorisation is sought and whether the activity can be undertaken within a shorter time frame.
- 7.17 The Authorising Officer should only authorise the activity that is the least intrusive in the circumstances. Any unnecessary intrusion, including collateral intrusion, must be minimised as much as practically possible. **The least intrusive method will be considered proportionate by the Courts.**
- 7.18 The Authorising Officer must balance the intrusiveness of the activity on

the target and others who might be affected by it against the need for the activity in operational terms. The Authorising Officer should discuss the proposed activity, and any proposed changes, with the applicant and/or the Senior Responsible Officer prior to issuing the authorisation.

8. CONSIDERING APPLICATIONS FOR THE USE OF A CHIS

- 8.1 This part of the Policy lists the factors which Authorising Officers should consider upon receiving an application for an authorisation for the use of a CHIS.

Step 1: Is Authorisation needed for this activity?

- 8.2 An Authorising Officer must first consider whether an authorisation is actually required. To require authorisation, the activity to which the application relates must be covert and must involve the obtaining of private information on an individual through the use of a CHIS.
- 8.3 An Authorising Officer should interpret the definitions broadly when determining whether an activity is covert or if private information will be obtained. When in doubt, the authorisation procedure must always be followed.
- 8.4 **At no time can an Authorising Officer authorise any intrusive surveillance.**

Step 2: Is the activity necessary?

- 8.5 An Authorising Officer can only authorise an activity where s/he believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing or detecting crime or of preventing disorder.
- 8.6 The Authorising Officer must be satisfied that there are no other reasonable means of carrying out the investigation, or obtaining the desired information, without undertaking the activity for which authorisation is sought.
- 8.7 Authorisation should not be granted if the information sought can be obtained by other means without undertaking an activity which falls under the requirements of RIPA.

Step 3: Is it proportionate?

- 8.8 If the activity is necessary, the Authorising Officer must also believe that the activity is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the activity against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the particular circumstances or if the information sought could reasonably be obtained by less intrusive means. Any activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair.

- 8.9 An Authorising Officer should first consider the following primary factors in determining whether the activity for which authorisation is sought is proportionate:

Confidential Information

- 8.10 The Authorising Officer must take into account the likelihood of confidential information being acquired. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

- 8.11 Where confidential information is likely to be acquired, authorisation should only be given in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

- 8.12 In these circumstances, the Authorising Officer must be Head of Paid Service or Senior Responsible Officer (exceptional circumstances).

8.13 Use of vulnerable persons as CHIS

- 8.14 When considering applications for the use of a CHIS, an Authorising Officer must determine whether the CHIS is a vulnerable individual or a juvenile in accordance with the following:

- The Authorising Officer must take into account the provisions of section 29 of RIPA and the Regulation of Investigatory Powers (Source Records) Regulations (2000 SI No. 2725) made under it before authorising the conduct or use of a CHIS.
- Section 29(5) requires the Authorising Officer to be satisfied that arrangements are in place for the careful management of the source and that records are maintained relating to the source which contain the particulars specified in the Source Records Regulations.

- 8.15 The Authorising Officer must therefore:

- be satisfied that the conduct and/or use of the CHIS is both necessary and proportionate to what is sought to be achieved. This will be addressed by following the procedure provided in this section;
- be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. This must address health and safety issues through a risk assessment;
- consider the likely degree of intrusion of all those potentially affected;

- consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and
 - ensure records contain specified particulars relating to the source and that the records are kept confidential.
- 8.16 In these circumstances, the Authorising Officer must be the Head of Paid Service or Senior Responsible Officer (exceptional circumstances).
- 8.17 Special safeguards apply to the use or conduct of vulnerable individuals or juveniles. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who may need protecting from exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional circumstances.
- 8.18 Use of juvenile covert human intelligence sources (JCHIS) is governed by Regulation of Investigatory Powers (Juveniles) Order 2000 as amended by the Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018.
- 8.19 A JCHIS is any source aged under 18, however further restriction apply when the JCHIS is under 16.
- 8.20 The Authorising Officer when considering the authorization must consider the statutory duty of the Council, under s11 of the Children Act 2004, to discharge its duties in a way that promotes and safeguards the welfare of children.
- 8.21 No authorisation may be granted for the conduct or use of a JCHIS; if the JCHIS is under the age of 16, and the relationship to which the conduct or use would relate is between the JCHIS and his parent or any person who has parental responsibility for them.
- 8.22 Where the Council intends to use a JCHIS under the age of 16 must ensure there is an appropriate adult at meetings with the JCHIS. An “appropriate adult” means:
- “(a) the parent or guardian of the source; or
 (b) any other person who has for the time being assumed responsibility for his welfare or is otherwise qualified to represent the interests of the source.”
- 8.23 No Authorisation may be granted or renewed for the use of a JCHIS (Under 18) unless the authorizing officer has undertaken or updated a risk assessment that demonstrates:

- the nature and magnitude of any risk of physical injury to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated; and
 - (the nature and magnitude of any risk of psychological distress to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated
- 8.24 An authorization for the use of a JCHIS may only be granted for a period of 4 months and is subject to monthly reviews.
- 8.25 A juvenile is a young person under 18. Juveniles can only be authorised as sources for four months. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or anyone with parental responsibility for that child.
- 8.26 Before deciding on this course of action, legal advice must be sought from the Chief Solicitor as the SRO.
- 8.27 When the proposed activity involves the use of a vulnerable person or juvenile as a CHIS, only the Head of Paid Service or in exceptional circumstances the Senior Responsible Officer

Risk of Collateral Intrusion

- 8.28 The Authorising Officer must consider whether there is a risk of collateral intrusion into the private life of any person not the primary subject of the investigation. The applicant should describe the activity sufficiently widely to include not only named individuals but also any others who may be at risk of collateral intrusion to enable this consideration to occur.
- 8.29 Where the risk of such intrusion is sufficiently significant, the Authorising Officer must determine whether a separate authorisation is required in respect of these other persons.
- 8.30 The person carrying out the activity must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation needs to be amended and re-authorised or a new authorisation is required.
- 8.31 The following further considerations must then be considered in determining whether the activity for which authorisation is sought is proportionate:
- The reasons given by the applicant as to why that activity is sufficient and adequate for obtaining the information sought;
 - Whether there are any other reasonable means of obtaining the information

sought;

- Whether the surveillance is an essential part of the investigation;
- The type and quality of the information the activity will produce and its likely value to the investigation;
- The amount of intrusion, other than collateral intrusion, the activity will cause and whether there are ways to authorise that intrusion; and
- The length of time for which the authorisation is sought and whether the activity can be undertaken within a shorter time frame.

8.32 The Authorising Officer should only authorise the activity that is the least intrusive in the circumstances. Any unnecessary intrusion, including collateral intrusion, must be authorised as much as practically possible. **The least intrusive method will be considered proportionate by the Courts.**

8.33 The Authorising Officer must balance the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The Authorising Officer should discuss the proposed activity, and any proposed changes, with the applicant and/or the Senior Responsible Officer prior to issuing the authorisation.

8.34 The Authorising Officer should discuss the proposed activity, and any proposed changes, with the applicant and/or the Senior Responsible Officer prior to issuing the authorisation.

9. **APPLYING FOR JUDICIAL APPROVAL**

9.1 Once an authorisation has been granted, the Senior Responsible Officer will review the authorisation paperwork to ensure that the authorisation fulfils the RIPA requirements and is necessary and proportionate. If satisfied that the surveillance is an appropriate use of the RIPA powers the Senior Responsible Officer (or an appointed representative of the Legal Division) will make an application to the Magistrates' Court to apply to have the authorisation approved/renewed by a Justice of the Peace.

9.2 The procedure for obtaining judicial approval is set out in the Home Office Guidance 'Protection of Freedoms Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000' published in October 2012. A flowchart setting out the procedure for obtaining Judicial Approval is set out at Appendix 1

9.3 The application form for Judicial Approval is appended to the guidance and available at the link below
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

10. ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

- 10.1 The provisions that govern the acquisition and disclosure of communications data are contained within IPA 2016. The IPA 2016 repealed the provisions relating to the interception and acquisition of communications data contained in RIPA 2000.
- 10.2 The Council is not able to authorise its own applications for the acquisition of communication data, which must be authorised by the OCDA. In order to make an application section 73 of the IPA, required the Council to be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services.
- 10.3 The Council's acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Article 8 (the right to respect for privacy and family life) and, in certain circumstances, Article 10 (right to freedom of expression) of the European Convention on Human Rights only if the conduct being authorised or required to take place is:
- Necessary for the purposes of a specific investigation or operation; and
 - Proportionate
- 10.4 When applying for authorisation to acquire communications data, the Council must believe the acquisition is necessary for the purpose of the prevention or detection of serious crime.
- 10.5 For the purpose of the IPA 'Serious crime' means:
- 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;
 - any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.
- 10.6 The Council must also believe the acquisition to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances.

11. AUTHORISATION TO ACCESS COMMUNICATIONS DATA

- 11.1 The applicant is a Council officer involved in conducting or assisting an investigation or operation who makes an application in writing or electronically

for the acquisition of communications data.

11.2 An application to acquire communications data must:

- a. describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)
- b. specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- c. include a unique reference number;
- d. include the name and the office, rank or position held by the person making the application;
- e. 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;
- f. include the operation name (if applicable) to which the application relates;
- g. identify and explain the time scale within which the data is required;
- h. explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- i. present the case for the authorisation in a fair and balanced way. 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 meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- j. consider and, where appropriate, describe any possible unintended
- k. consequences of the application; and
- l. where data is being sought from a telecommunications operator or postal
- m. operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

11.3 The Council is required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

11.4 In addition to involving the NAFN SPoC, the Council must ensure that someone – “the verifying officer” – of at least the rank of the Council’s SRO is aware the application is being made before it is submitted to an authorising officer in OCDA.

11.5 It is the duty of the senior responsible officer in a public authority to ensure that the public authority makes available to the SPoC and the authorising individual such information as the senior responsible officer thinks necessary

to ensure the integrity of any requirements for the acquisition of entity data to be obtained directly upon the acquisition or disclosure of any events data, and their compliance with Part 3 of the IPA and with this code of practices.

- 11.6 NAFA SPoC will submit the application
- 11.7 Where a request is refused by an authorising officer in OCDA, the Council has three options:
- not proceed with the request;
 - resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data;
 - resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.
- 11.8 Where an application is granted the NAFA SPoC would normally be the person who takes receipt of any communications data acquired from a telecommunications operator or postal operator and would normally be responsible for its dissemination to the applicant within the Council.
- 11.9 The Council must cease any and all authorised acquisition of communications data as soon as the OCDA authorisation is cancelled or at the expiry of one month following the date of authorisation (whichever is sooner).

12. WORKING WITH/THROUGH OTHER AGENCIES

- 12.1 Where Council Officers undertake an investigation/operation under RIPA jointly with another public authority, it is the responsibility of the tasking authority to obtain the authorisation. For example, if the Council was asked by the Police to assist in a covert surveillance operation, the Police should obtain the authorisation, which would then cover the Council. In such a case, Council Officers must request written confirmation from the other public authority that an authorisation is in place before taking part in any joint operation.

13. RECORDS MANAGEMENT

- 13.1 The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in the relevant services. A central record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the RIPA Co-ordinator.
- 13.2 All Authorising Officers must send all applications for authorisation to the

RIPA Co-ordinator within 2 working days of issue of signature. Each document will be given a unique reference number, a copy will be placed on the Central Record and the original will be returned to the applicant.

- 13.3 Copies of all other forms used must be sent to the RIPA Co-ordinator bearing the reference number previously given to the application to which it refers.
- 13.4 The RIPA Coordinator shall retain all records in accordance with the Council's Retention schedule for a period of 6 years for the date the authorization

Service Records

- 13.5 Each service must keep a written record of all authorisations issued to it, to include the following:
- A copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
 - A record of the period over which the surveillance has taken place;
 - The frequency of reviews prescribed by the Authorising Officer;
 - A record of the result of each review;
 - A copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;
 - The date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation.

Central Record Maintained by the RIPA Co-ordinator

- 13.6 A central record of all authorisation forms, whether authorised or rejected, is kept by the RIPA Co-ordinator. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner's Office.
- 13.7 The central record must be updated whenever an authorisation is granted, renewed or cancelled. Records will be retained for a period of 3 years from the date on which the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the internal procedures relating to the retention of the criminal or civil proceedings file.
- 13.8 The central record must contain the following information:
- The type of authorisation;
 - The date on which the authorisation was given;
 - name/rank of the Authorising Officer;
 - The unique reference number (URN) of the investigation/operation. This will be issued by the Legal Division when a new application is entered in the Central Record. The applicant will be informed accordingly and should use the same URN when requesting a renewal or cancellation;
 - The title of the investigation/operation, including a brief description and names of the subjects, if known;
 - If the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;
 - Whether the investigation/operation is likely to result in the obtaining of

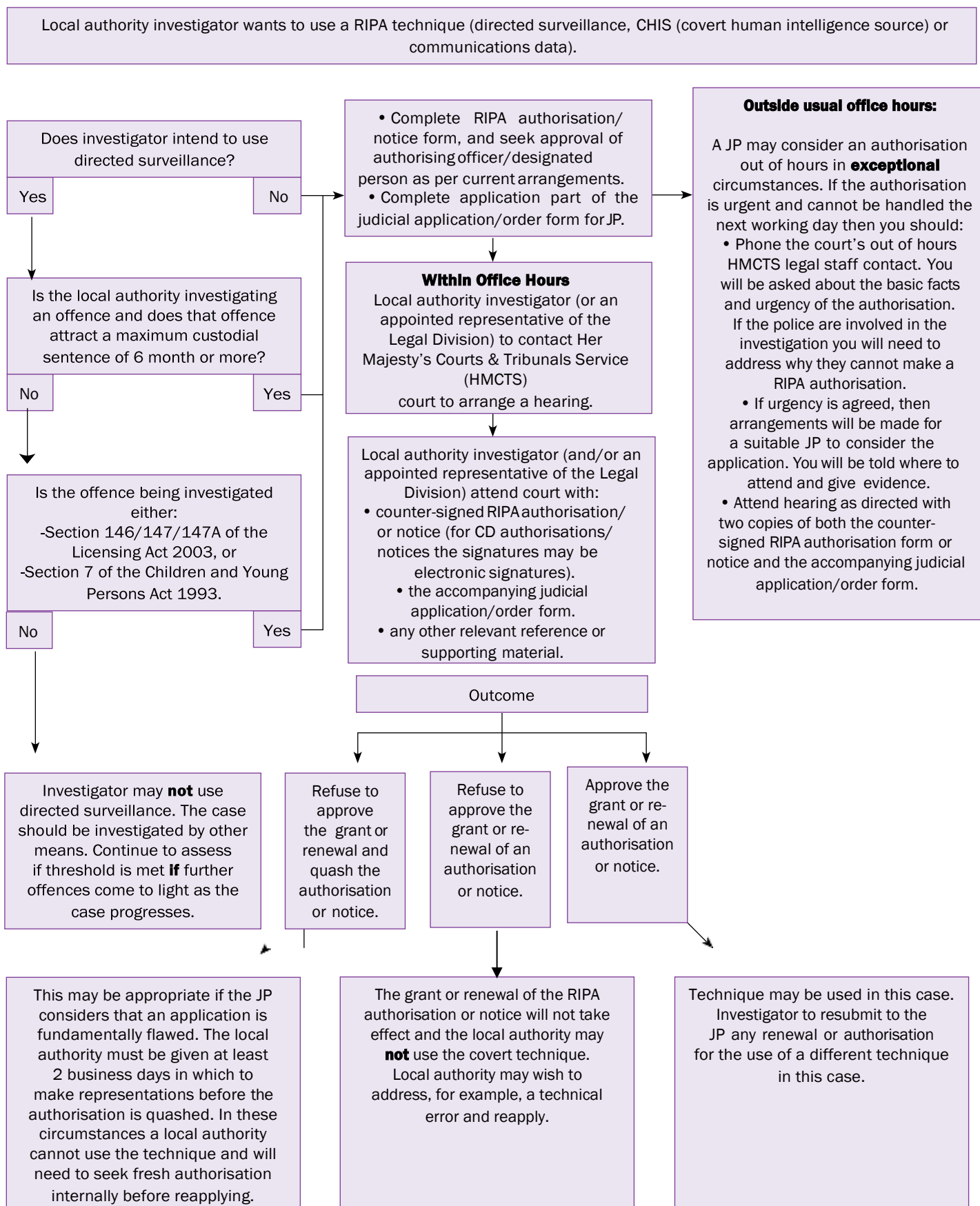
- confidential information; and
- The date and time that the authorisation was cancelled.

Retention and Destruction of Material

- 13.9 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Material obtained is likely to include the following;
- Recordings of direct surveillance,
 - Notes of offices undertaking surveillance, and
 - Emails and other communications (including attendance notes of telephone calls reference the above.
- 13.10 Duplication of direct records should be keep the minimum and only undertaken, where necessary for the efficient conduct of the investigation or prosecution.
- 13.11 Other information will inevitably be duplicated as part of an investigation as part of routine case discussions between investigating officers, managers and legal services. This information will likely be stored within the Council's outlook email system, but may also include duplicates contained within personal files individuals involved, both on the Council network and locally on individual devices.
- 13.12 Departments must ensure that other duplicate of information are permanently delated or securely disposed at the conclusion of an investigations. The Department should ensure that there is one complete file for archive at the conclusion of the investigation, this will be sorted electronically on a secure area of the HBC network with access limited to those individuals with need of access.
- 13.13 This may involve liaison with legal services, where advice has been sought but not prosecution of other action undertaken. In this situation department should inform the legal services the investigation is at an end and requesting any information is deleted unless sorted within open file.
- 13.14 Where a file has been opened by legal services a separate copy of the material be stored within that file. As with instructing departments, legal services must ensure there is only one complete file is retained at the conclusion of proceedings and that other duplicates are deleted or surely disposed of once the file is closed for archive(this may be either electronic or in hard copy).
- 13.15 Archived files should be sorted in accordance with the Council's retention schedule a copy of which is available on the council intranet.
- <http://hbcintranet/Pages/Information%20Governance/Information-Governance-Policies.aspx>
- 13.16 Where there is doubt, advice must be sought from the Senior Responsible Officer or in their absence the RIPA Co-ordinator.

APPENDIX 1

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Obtain signed order and retain original RIPA authorisation/notice.

For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.

If out of hours, a copy of the signed order to be provided to the court the next working day.



RIPA PROCEDURE FOR E-CRIME, INCLUDING INVESTIGATION OF SOCIAL NETWORKING SITES

1. Introduction

Many enquiries relating to goods or services bought online will be simple investigations where a website is acting as a shop providing products. It is unlikely that such investigations will invoke a need for authorisations under RIPA because: -

1. The owners of the website can have no reasonable prospect of privacy;
2. The site is unlikely to contain private information; and
3. It is unlikely that a relationship will be established between the seller and the user of the site if a single purchase is made or if the number of visits to the site is limited to those necessary to secure evidence in relation to the product or practice complained about.

Social Networking sites create different issues as the whole purpose of the sites, is on the face of it, to create the opportunities to set up social networks and thus create relationships. These sites, such as Facebook, Twitter, LinkedIn, Pinterest, Beebo and Snapchat have different levels of privacy, but it is likely that, even at the most open and accessible level, personal information about those maintaining the site or pages or posting information will be available. Whilst it could be argued that those who make such information freely available can have no expectation that it will remain private, it is also likely that they do not expect that it will be read and retained by an investigator. This activity is analogous to private activity occurring in a public place, and, as in the real world, if such activity were observed as a planned activity by an investigator, an authorisation for directed surveillance would be required.

Surveillance is defined in Section 48 of the Regulation of Investigatory Powers Act 2000 (RIPA) as including: -

- (a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- (b) recording anything monitored, observed or listened to in the course of surveillance; and
- (c) surveillance by or with the assistance of a surveillance device.

It could be argued that this definition could be interpreted so as to exclude monitoring of social networking sites as the people under surveillance are not present or visible to the investigators. However, if we go back to the Human Rights Act and the Convention Rights, namely Article 8 (Everyone has the right to respect for his private and family life, his home and his correspondence), and Article 10 (Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers), there is likelihood that uncontrolled and unconsidered access to personal social

networking sites will breach these rights. As these rights are qualified rights, in that they can be infringed for certain purposes, it is appropriate that authorisation under RIPA is sought for surveillance of such sites.

The principles in this Policy should also be considered when monitoring business websites, such as eBay, which are used by non-trade people to advertise products. It is likely that a general viewing of eBay would include some collateral intrusion, but this is minimal and is likely to be proportionate in the context of the crime being investigated.

This Policy should be read in conjunction with the wider Hartlepool Borough Council RIPA Policy. The provisions in that Policy will apply along with the specific Policy outlined in this document.

2. Initial activity

The relevant dictionary definition of 'monitor' (namely, 'to maintain regular surveillance over') suggests an act undertaken either on more than one occasion or for more than a short period of time. This explicitly suggests that an initial visit to a website is not surveillance, nor would a repeat visit be if the second visit were not close in time to the first one.

Before an investigator visits a site they should consider what information they are seeking and what information is likely to be found. The focus should be on collecting evidence to prove, or disprove, any wrongdoing. If an investigation involves more than one Officer or is being conducted by the Authority and other partners, one Officer should be identified to undertake one initial visit and they alone should carry it out. Any other Officers, including partners, who will undertake surveillance as part of the investigation should be identified on the application for authorisation.

Once this initial visit to the site is completed, the Officer should consider whether further visits are necessary or if sufficient evidence has been secured for the next steps in the investigation (e.g. an application for a warrant) to take place. If it is decided that further monitoring of the social networking site is to take place, it should be assumed that an authorisation for directed surveillance will be needed. If the investigator does not believe that further visits require an authorisation they should record their reasons and discuss the matter with their manager who will, in turn discuss it with their Unit Manager.

3. When authorisation is required

It is clear that frequent and/or extended visits would be classed as surveillance and an authorisation for directed surveillance under RIPA should be sought if the investigator intends to carry out such monitoring activity. The OSC Guidance, at paragraph 124 states that 'present monitoring could be of past events.' This could occur if investigators look at the timeline on a target's site to, for example, establish a lifestyle pattern or to identify relationships.

Any application for directed surveillance should be submitted promptly, while the evidence obtained is still current. The application should have regard to necessity, proportionality and the likelihood of collateral intrusion as for any other directed surveillance application, recognising that the factors to be taken into account will be different to those that exist off-line.

4. Necessity

Any application for an authorisation under the Act will be for the prevention or detection of crime. The investigator will need to show that there is a need to collect evidence, to identify

what type of evidence is likely to be collected; its value to the investigation and that surveillance of the social networking site is the only way to collect it. Any information on other means of obtaining the evidence should be included, if such means have been identified, along with an explanation of why it is necessary to use directed surveillance and not those other means.

5. Proportionality

The investigator will need to show that the scale of the crime being investigated justifies the potential intrusion into the target's private life. For example, it may not be proportionate to conduct surveillance into someone who has infrequently sold items at a level that would be regarded as below a trading threshold. Investigators should have reasonable grounds to suspect that the target is actively committing serious breaches of legislation that are more than technical or minor.

Note: since the coming into force of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 the authority can only authorise directed surveillance where the offence being investigated is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment or is an offence involving sales of alcohol or tobacco to children.

6. Collateral Intrusion

It is likely that collateral intrusion into the activities or comments of those persons who are interacting with the target individuals will take place. This intrusion will need to be tightly managed as far as is possible. It is also possible that family members' information will be posted on the site, especially on the target's individual Facebook pages. This will be treated in the same way as other information acquired that is identified as not being relevant to the investigation.

For public protection, the primary target of surveillance is likely to be business and group pages used primarily for selling goods or those who we believe are repeatedly committing serious environmental crimes. These sites are less likely to contain personal information but it cannot be ruled out. As part of the application for authorisation for directed surveillance, investigators should identify the likelihood of collateral intrusion. This will be supported by any evidence acquired during the initial visit to the site.

Any information about individuals, groups or business believed not to be engaged in criminal activity will be extracted from the evidence. This process will involve the investigating officer consulting their manager and a decision being made on each piece of information gathered. Where the information gathered does not relate to any suspected criminal activity, the information will be given a unique reference number and a record kept of the reason for the decision that the information is not relevant to enquiries. This information and the decision records will then be stored securely for inspection and audit purposes only by authorised personnel from the Office of the Surveillance Commissioner.

If the evidence collected shows that the business profiles and group forums are established closed groups, enabling the commission of relevant crimes, it follows that other members of the pages may also be investigated, to eliminate or identify them as a subject of interest. Consideration will be given to the need to obtain further authorisations under the Act, before any surveillance is conducted against other associated users.

Collateral intrusion could also include personal information collected about people other than the target. This information may be included in written, pictorial, video and audio form. Some of this information may be needed to identify others committing offences or assisting the principal in any relevant way, where it had not already been obtained. The evidence may also provide a connection between the website, the activity and any physical premises. If it is likely that this information will be encountered, or if it is needed to identify the target, explicit reference to it must be made in any application for authorisation and reasons for collecting it should be given.

7. Practical Matters

The Trading Standards stand-alone computer should be used, using the fake identity already established, wherever possible, or failing that, the Officer's own password protected NCC issued computer. Evidence of any offences should be secured by using hypercam or webreaper software, if possible, or by screen dump printing if not. Monitoring should not be carried out on an Officer's own computer, nor should monitoring take place outside of working hours, unless the particular circumstances of the investigation require it. Those circumstances will be included in any application for surveillance.

A log shall be kept of all surveillance activity, showing the date of the surveillance, the operation name, the start and finishing times and the sites visited. The application for authorisation should include this information where possible or the application should include the parameters within which the surveillance activity will take place. This will allow us to show that any activity undertaken is authorised.

Investigators should also be aware that the site could contain violent or pornographic images or information, or information of a politically extremist nature. If such images or information are found, the investigator should record details of web address of the site that was visited and how the site was accessed (some sites may be displayed even if the investigator did not intend it). The investigator should discuss the matter with their manager who should consider if there is a need to contact any other enforcement or safeguarding agency.

8. Cancellation of Authorisations

Any authorisation to conduct directed surveillance on an individual's page or site should be cancelled as soon as it is no longer needed. This is likely to occur when sufficient evidence to proceed to the next stage of the investigation has been secured or if monitoring of the page or site has revealed no criminal activity. Authorisations to monitor activity on social media sites are subject to the same review procedures as applications for real life surveillance. The review will determine if the authorisation is still necessary, proportionate and if the likelihood and level of collateral intrusion have changed since the authorisation was initially applied for.

9. Other matters

This Policy does not include 'befriending' or similar activity. This is a reflection of the fact that most sellers and their activities can be identified as part of open source research and items are sold from accessible websites. Befriending may require authorisation for an officer to act as a Covert Human Intelligence Source within the meaning of Part III of the Act. Further policies will be developed if market practices change such that investigators identify the need for such authorisations in relation to social networking sites.

10. Further Guidance

Further guidance is available from the Office of the Surveillance Commissioners Procedures and Guidance published in July 2016 which states at paragraphs 239 and 289: -

Covert Internet Investigations - e-trading

239 CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage.

Covert surveillance of Social Networking Sites (SNS)

289 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

Selected comments from The Surveillance Commissioner's Report for 2015/2016 (Numbers refer to paragraphs in the report)

The “virtual world”

2.8. There is a discernible shift towards criminal activity in or by the use of what I may describe as the —virtual world this increases the demands on those responsible for covert surveillance. They need an understanding of the technological advances and myriad types of communication and storage devices which are constantly being updated. They also need assistance about how the statutory powers available to them can or should be applied to technological developments of which criminals take advantage, factoring in potential regional, national or international boundaries. The developments, complex as they can be, do not diminish the requirement that any surveillance activity can only be undertaken in accordance with the provisions of the relevant authorisation.

Social Networks and the “virtual world”

5.17. Patterns of criminal planning are changing to embrace technological advances. Criminals and terrorists are less likely to meet in public, in parked up cars, with police officers using binoculars and longsighted cameras to follow their movements. Social media and private electronic communications provide greater anonymity for the criminals, and enable their activities to proceed on a global scale. This issue was addressed by my predecessor in his last two reports, and the Surveillance Commissioners have issued guidance on the need for appropriate authorisations to cover these developments.

5.18. My Inspectors and the Assistant Surveillance Commissioners pay particular attention to the way this developing method of criminal activity is kept under covert surveillance. The topic forms the basis for numerous requests for guidance. Perhaps the most significant feature is that investigating authorities cannot proceed on the basis that because social networking developed after much of the legislation came into force it is immunised from compliance with it. Requirements for appropriate authorisation may arise from the work done by those whose roles do not traditionally fall within RIPA or RIP(S)A. The necessary training and information must be addressed by the Senior Responsible Officer in each authority.

5.19. Two examples illustrate the issues.

Example 1: In one particular public authority, once a task is allocated to an internet desk Officer, that Officer undertakes research using a non-attributable computer which stands alone from the authority's main network. Although it is said that the staff do not use false personas, the activity they undertake is calculated to be covert so as to minimise the risk of compromise to ongoing investigations. Staff typically undertake research on one occasion, although this singular research activity may extend over several hours and involve research of different social media sites linked to the subject. There is a perception by staff within the unit that investigators are reluctant to, or dissuaded from, making more than one request for research to be undertaken on the same subject. The head of the unit believes that investigators are missing opportunities for securing valuable intelligence by restricting their request to singular research; this is a view shared by the inspection team. Very rarely are any requests for research of open source material or social media supported by an authorisation for directed surveillance. In a twelve month period the unit has processed 3,561 requests for internet research, on just two occasions directed surveillance authorisations supported the activity being undertaken.

Example 2: In another public authority, one matter absent from the various policy and guidance documents is the use of the internet for investigative purposes. This technique of investigation and research is expanding exponentially with all manner of new

technology and although some knowledge and awareness was evident during discussion with staff, further guidance and advice would benefit investigators and Authorising Officers alike. The key consideration when viewing publicly available information where no privacy settings have been applied, often referred to as 'open source' material, is the **repeated** or **systematic** collection of private information. Initial research of social media to establish a fact or corroborate an intelligence picture is unlikely to require an authorisation for directed surveillance; whereas repeated visits building up a profile of a person's lifestyle would do so. Each case must be considered on its individual circumstances and early discussion between the investigator and the Authorising Officer is advised to determine whether activity should be conducted with or without the protection of an authorisation.

5.20. Part of their inspections of councils, the Inspectors and Assistant Surveillance Commissioners discuss with appropriate officials, and frequently undertake visits to examine the CCTV facilities which they manage. It is very rare for a council to authorise directed surveillance which includes the use of its CCTV system, but occasionally others, for example the local police force, may wish to do so, as part of covert rather than routine overt surveillance. When this arises, there should be a written protocol in place between the council, as owners or managers of the system, and the body which seeks to use it in a covert manner, so as to ensure that the lines of responsibility are clearly understood, and appropriate arrangements for authorisation are then made.

STRICTLY PRIVATE & CONFIDENTIAL

HARTLEPOOL BOROUGH COUNCIL

NON- RIPA AUTHORISATION FORM

Non-RIPA Form to address issues of necessity and proportionality before carrying out surveillance of staff or others which falls outside the remit of RIPA

Guidance Note:

1. Only officers who would be authorised under RIPA can sign the form Applicants and authorised officers must comply, in full, with the Human Rights Act 1998. If in doubt contact Hayley Martin, 01429 523002.
2. Completed forms should be forwarded to Amanda Whitaker, RIPA Co-ordinator.
3. All boxes in this form must be completed. Not applicable, n/a or lines must be put through irrelevant boxes.

Subject of Surveillance (including full address)		Unique Reference Number (URN)/Operation Name:	Year/Service/Number/Name
--	--	---	--------------------------

SECTION 1 (to be completed by the applicant)

Name of Applicant		Service	
Full Address			
Contact Details			
Investigation/ Operation Name (if applicable)			

Details of application:

1. Give name / job title of authorised officer:

2. Describe the purpose of the surveillance.

3. Describe, in detail, the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used:

4. The identities, where known, of those to the subject of the surveillance:

- Name:
- Address:
- DOB:
- Other known / relevant information:

5. Explain the information that is desired to obtain as a result of the surveillance:

6. Explain <u>why</u> surveillance is <u>NECESSARY</u> in this particular case:
-

7. Supply details of any potential <u>COLLATERAL</u> INTRUSION and why the intrusion is unavoidable: (Also describe precautions to MINIMISE collateral intrusion)

8. Explain <u>why</u> the surveillance is PROPORTIONATE to what it seeks to achieve. However intrusive might it be or the subject of surveillance or on others? Any why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

9. Applicant's Details	
Name (print)	Tel No:
Job Title	Date
Signature	

Authorising Officers considerations of necessity and proportionality

Authorising Officers Signature

.....

Date

.....

AUDIT AND GOVERNANCE COMMITTEE

29 SEPTEMBER 2022



Report of: Chief Solicitor and Monitoring Officer

Subject: TEES VALLEY JOINT HEALTH SCRUTINY
COMMITTEE – OUTSIDE BODY RESIGNATION

1. PURPOSE OF REPORT

- 1.1 To seek the appointment of a replacement Member to the Tees Valley Joint Health Scrutiny Committee following the resignation of Councillor Falconer.

2. BACKGROUND

- 2.1 The Tees Valley Joint Health Scrutiny Committee comprises of the following local authorities, Hartlepool Borough Council, Stockton on Tees Borough Council, Redcar and Cleveland Borough Council and Darlington Borough Council. The Committee facilitates the exchange of information about planned health scrutiny work and shares information and outcomes from local health scrutiny reviews.
- 2.2 The Committee also considers proposals for scrutiny of regional or specialist health services in order to ensure that the value of proposed health scrutiny exercises is not compromised by lack of input from appropriate sources and that the NHS is not over-burdened by similar reviews taking place in a short space of time. A full copy of the Committee's Terms of Reference is attached at Appendix A.
- 2.3 The administration of the Joint Committee is rotated annually across the local authorities involved and for 2022/23 this responsibility sits with Darlington Borough Council who will also provide the Chair for the Committee. The Committee will meet quarterly at 10.30 am in the Council Chamber, Darlington Town Hall on the following dates:
- Friday 23rd September 2022
 - Friday 16th December 2022
 - Friday 17th March 2023

- 2.4 The membership of the Tees Valley Joint Health Scrutiny Committee consists of three Members from each Local Authority and the following appointments were made by Annual Council on 24 May 2022:

- **Councillor Cook (Chair of Audit and Governance)**
- **Councillor Creevy (Labour)**
- **Councillor Falconer (Conservative and Independent Union)**

3. PROPOSALS/ISSUES FOR CONSIDERATION

- 3.1 Following the recent resignation of Councillor Falconer from her position on this body, a replacement Conservative and Independent Union Member is sought.

4. RECOMMENDATIONS

- 4.1 The Committee is requested to appoint a replacement Conservative and Independent Union Member to the Tees Valley Joint Health Scrutiny Committee.

5. BACKGROUND PAPERS

- 5.1 HBC Constitution Part 7; Appointments to Outside organisations and other bodies.

6. CONTACT OFFICER

- 6.1 Hayley Martin, Chief Solicitor and Monitoring Officer
Legal Services Department
Hartlepool Borough Council
Tel 01429 523002
Email: hayley.martin@hartlepool.gov.uk

- 6.2 Denise Wimpenny, Principal Democratic Services Officer
Legal Services Department
Hartlepool Borough Council
Tel 01429 523193
Email: denise.wimpenny@hartlepool.gov.uk

Appendix A

Protocol / Terms of Reference for the Tees Valley Health Scrutiny Joint Committee

1. This protocol provides a framework for carrying out scrutiny of regional and specialist health services that impact upon residents of the Tees Valley under powers for local authorities to scrutinise the NHS outlined in the NHS Act 2006, as amended by the Health and Social Care Act 2012, and related regulations.
2. The protocol will be reviewed as soon as is reasonably practicable, at the start of each new Municipal year. Minor amendments to the protocol that do not impact on the constitutions of the constituent Tees Valley Authorities will be determined by the Joint Committee at the first meeting in each Municipal year. An amended protocol, following agreement from the Tees Valley Health Scrutiny Joint Committee will be circulated for information to:-

Tees Valley Local Authorities

3. Darlington; Hartlepool; Middlesbrough; Redcar and Cleveland; Stockton-on-Tees (each referred to as either an “authority” or “Council”).

NHS England Area Teams

4. Durham, Darlington and Tees Area Team

NHS Foundation Trusts

5. County Durham and Darlington Trust; North Tees and Hartlepool Trust; South Tees Hospitals Trust; Tees, Esk & Wear Valleys NHS Trust; North East Ambulance Service.

Clinical Commissioning Groups

6. Darlington; Hartlepool and Stockton-on-Tees; South Tees;

Tees Valley Health Scrutiny Joint Committee

7. A Tees Valley Health Scrutiny Joint Committee (“the Joint Committee”) comprising the five Tees Valley Authorities has been created to act as a forum for the scrutiny of regional and specialist health scrutiny issues which impact upon the residents of the Tees valley and for sharing information and best practice in relation to health scrutiny and health scrutiny issues.

Membership

8. When holding general meetings, the Joint Committee will comprise 3 Councillors from each of the Tees Valley Local Authorities (supported by appropriate Officers as necessary) nominated on the basis of each authority’s

- political proportionality, unless it is determined by all of the constituent Local Authorities that the political balance requirements should be waived.
9. The terms of office for representatives will be one year from the date of their Authority's annual council meeting. If a representative ceases to be a Councillor, or wishes to resign from the Joint Committee, the relevant council shall inform the Joint Committee secretariat and a replacement representative will be nominated and shall serve for the remainder of the original representative's term of office.
 10. To ensure that the operation of the Joint Committee is consistent with the Constitutions of all Tees Valley Authorities, those Authorities operating a substitution system shall be entitled to nominate substitutes. Substitutes (when not attending in place of the relevant Joint Committee member, and exercising the voting rights of that member) shall be entitled to attend general or review meetings of the Joint Committee as non-voting observers in order to familiarise themselves with the issues being considered.
 11. The Joint Committee may ask individuals to assist it on a review by review basis (in a non-voting capacity) and may ask independent professionals to advise it during a review.
 12. The quorum for general meetings of the Joint Committee shall be 6, provided that 3 out of 5 authorities are represented at general meetings. The quorum for Tees-wide review meetings, in cases where some Authorities have chosen not to be involved, shall be one third of those entitled to be present, provided that a majority of remaining participating authorities are represented. Where only 2 authorities are participating both authorities must be represented.
 13. The Joint Committee will conduct health reviews which impact upon residents of the whole of the Tees Valley. If however one or more of the Councils decide that they do not wish to take part in such Tees-wide reviews, the Joint Committee will consist of representatives from the remaining Councils, subject to the quorum requirements in paragraph 12.
 14. Where a review of a 'substantial development or variation' will only affect the residents of part of the Tees Valley, Councils where residents will not be affected will not take part in any such review. In such cases, the Joint Committee will liaise with the Councils where residents will be affected, in order to assist in establishing a separate joint body (committee) to undertake the review concerned. The composition of the committee concerned may include representatives from other Local Authorities outside the Tees Valley, where the residents of those Authorities will also be affected by the proposed review. The chairmanship, terms of reference, member composition, procedures and any other arrangements which will facilitate the conducting of the review in question will be matters for the joint body itself to determine.
 15. It is accepted, however, that in relation to such reviews, the relevant constituent authorities of the committee concerned may also undertake their own health scrutiny reviews and that the outcome of any such reviews will inform the final report and formal consultation response of the committee.

Chair and Vice-Chair

16. The Chair of the Joint Committee will be rotated annually between the Tees Valley Authorities in the following order:-

Stockton
Hartlepool
Redcar & Cleveland
Middlesbrough
Darlington

17. The Joint Committee shall have a Vice-Chair from the Authority next in rotation for the Chair. At the first meeting of each municipal year, the Joint Committee shall appoint as Chair and Vice-Chair the Councillors nominated by the relevant Councils. If the Chair and Vice-Chair are absent from a meeting, the Joint Committee shall appoint a member to act as Chair for that meeting. The Chair will not have a second or casting vote.
18. Where the Authority holding the Chair or Vice-Chair has chosen not to be involved in a Tees-wide review, the Chair and Vice-Chair of the Joint Committee for the duration of that review will be appointed at a general meeting of the Joint Committee.

Co-option of other local authorities

19. Where the Joint Committee is to conduct a Tees-wide scrutiny review into services which will also directly impact on the residents of another local authority or authorities outside the Tees Valley, that authority or authorities will be invited to participate in the review as full and equal voting Members.

Terms of Reference

20. The Joint Committee shall have general meetings involving all the Tees Valley authorities:-
- To facilitate the exchange of information about planned health scrutiny work and to share information and outcomes from local health scrutiny reviews;
 - To consider proposals for scrutiny of regional or specialist health services in order to ensure that the value of proposed health scrutiny exercises is not compromised by lack of input from appropriate sources and that the NHS is not over-burdened by similar reviews taking place in a short space of time.
21. The Joint Committee will consider any proposals to review regional or specialist services that impact on the residents of the whole Tees Valley area. The aim will be for the Joint Committee to reach a consensus on the issues to be subject to joint scrutiny, but this may not always be possible. In these circumstances

it is recognised that each council can conduct its own health scrutiny reviews when they consider this to be in the best interests of their residents.

22. In respect of Tees Valley-wide reviews (including consideration of substantial developments or variations), the arrangements for carrying out the review (eg whether by the Joint Committee or a Sub-Committee), terms of reference, timescale, outline of how the review will progress and reporting procedures will be agreed at a general meeting of the Joint Committee at which all Tees Valley Authorities are represented.
23. The Joint Committee may also wish to scrutinise services provided for Tees Valley residents outside the Tees Valley. The Joint Committee will liaise with relevant providers to determine the best way of achieving this.
24. The basis of joint health scrutiny will be co-operation and partnership within mutual understanding of the following aims:-
 - to improve the health of local people and to tackle health inequalities;
 - ensuring that people's views and wishes about health and health services are identified and integrated into plans and services that achieve local health improvements;
 - scrutinising whether all parts of the community are able to access health services and whether the outcomes of health services are equally good for all sections of the community.
25. Each Local Authority will plan its own programme of health scrutiny reviews to be carried out locally or in conjunction with neighbouring authorities when issues under consideration are relevant only to their residents. This programme will be presented to the Joint Committee for information.
26. Health scrutiny will focus on improving health services and the health of Tees Valley residents. Individual complaints about health services will not be considered. However, the Joint Committee may scrutinise trends in complaints where these are felt to be a cause for concern.

Administration

27. The Joint Committee will hold quarterly meetings. Additional meetings may be held in agreement with the Chair and Vice-Chair, or where at least 6 Members request a meeting. Agendas for meetings shall be determined by the secretariat in consultation with the Chair.
28. Notice of meetings of the Joint Committee will be sent to each member of the Joint Committee five clear working days before the date of the meeting and also to the Chair of the constituent authorities' relevant overview and scrutiny committees (for information). Notices of meetings will include the agenda and

papers for meetings. Papers “to follow” will not be permitted except in exceptional circumstances and as agreed with the Chair.

29. Minutes of meetings will be supplied to each member of the Joint Committee and to the Chairs of the constituent authorities’ relevant overview and scrutiny committees (for information) and shall be confirmed at the next meeting of the Joint Committee.
30. Meetings shall be held at the times, dates and places determined by the Chair.

Final Reports and Recommendations

31. The Joint Committee is independent of its constituent Councils, Executives and political groups and this independence should not be compromised by any member, officer or NHS body. The Joint Committee will send copies of its final reports to the bodies that are able to implement its recommendations (including the constituent authorities). This will include the NHS and local authority Executives.
32. The primary objective is to reach consensus, but where there are any matters as regards which there is no consensus, the Joint Committee’s final report and formal consultation response will include, in full, the views of all constituent councils, with the specific reasons for those views, regarding those matters where there is no consensus, as well as the constituent authorities’ views in relation to those matters where there is a consensus.
33. The Joint Committee will act as a forum for sharing the outcomes and recommendations of reviews with the NHS body being reviewed. NHS bodies will prepare Action Plans that will be used to monitor progress of recommendations.

Substantial Developments or Variations to Health Services

34. The Joint Committee will act as a depository for the views of its constituent authorities when consultation by local NHS bodies has under consideration any proposal for a substantial development of, or variation in, the provision of the health service across the Tees Valley, where that proposal will impact upon residents of each of the Tees Valley Local Authorities.
35. In such cases the Joint Committee will seek the views of its constituent authorities as to whether they consider the proposed change to represent a significant variation to health provision, specifically taking into account:-
 - changes in accessibility of services
 - impact of proposal on the wider community
 - patients affected
 - methods of service delivery
36. Provided that the proposal will impact upon residents of the whole of the Tees Valley, the Joint Committee will undertake the statutory review as required

under the Local Authority (Public Health, Health and Wellbeing Boards and Public Health) Regulations 2013. Neighbouring authorities not normally part of the Joint Committee, may be included where it is considered appropriate to do so by the Joint Committee. In accordance with paragraph 22, the Joint Committee will agree the arrangements for carrying out the Review.

37. Where a review does not affect the residents of the whole of the Tees Valley the provisions of paragraphs 14 and 15 will apply and the statutory review will be conducted accordingly.
38. In all cases due regard will be taken of the NHS Act 2006 as amended by the Health and Social Care Act 2012, and the Local Authority (Public Health, Health and Wellbeing Boards and Public Health) Regulations 2013.

Principles for Joint Health Scrutiny

39. The health of Tees Valley residents is dependent on a number of factors including the quality of services provided by the NHS, the local authorities and local partnerships. The success of joint health scrutiny is dependent on the members of the Joint Committee as well as the NHS.
40. The local authorities and NHS bodies will be willing to share knowledge, respond to requests for information and carry out their duties in an atmosphere of courtesy and respect in accordance with their codes of conduct. Personal and prejudicial and/or disclosable pecuniary interests will be declared in all cases in accordance with the code of conduct and Localism Act 2011.
41. The scrutiny process will be open and transparent in accordance with the Local Government Act 1972 and the Access to information Act 1985 and meetings will be held in public. Only information that is expressly defined in regulations to be confidential or exempt from publication will be considered in private and only if the Joint Committee so decide. Papers of the Joints Committee can be posted on the websites of the constituent authorities as determined by each authority.
42. Different approaches to scrutiny reviews may be taken in each case. The Joint Committee will seek to act as inclusively as possible and will take evidence from a wide range of opinion including patients, carers, the voluntary sector, NHS regulatory bodies and staff associations. Attempts will be made to ascertain the views of hard to reach groups, young people and the general public.
43. The Joint Committee will work to continually strengthen links with the other public and patient involvement bodies such as local HealthWatch.
44. The regulations covering health scrutiny require any officer of an NHS body to attend meetings of health scrutiny committees. However, the Joint Committee recognises that Chief Executives and Chairs of NHS bodies may wish to attend with other appropriate officers, depending on the matter under review. Reasonable time will be given for the provision of information by those asked to provide evidence.

45. Evidence and final reports will be written in plain English ensuring that acronyms and technical terms are explained.
46. The Joint Committee will work towards developing an annual work programme in consultation with the NHS and will endeavour to develop an indicative programme for a further 2 years. The NHS will inform the secretariat at an early stage on any likely proposals for substantial variations and developments in services that will impact on the Joint Committee's work programme. Each of the Tees Valley authorities will have regular dialogue with their local NHS bodies. NHS bodies that cover a wide geographic area (eg mental health and ambulance services) will be invited to attend meetings of the Joint Committee on a regular basis.
47. Communication with the media in connection with reviews will be handled in conjunction with each of the constituent local authorities' press officers.