AUDIT AND GOVERNANCE COMMITTEE

AGENDA

15th October 2024

at 5pm

in Council Chamber
Civic Centre, Hartlepool

MEMBERS: AUDIT AND GOVERNANCE COMMITTEE

Councillors Boddy, Buchan, Darby, Hall, Holbrook, Jorgeson, Moore, Morley, Roy and Thompson.

Standards Co-opted Independent Members: - Mr Martin Slimings.

Standards Co-opted Parish Council Representatives: Parish Councillor Kane Forrester (Wynyard) and Parish Councillor Patricia Andrews (Headland)

Local Police Representative

1. **APOLOGIES FOR ABSENCE**

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

3. **MINUTES**

None

4. **AUDIT ITEMS**

No Items

5. **STANDARDS ITEMS**

No Items

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.

6. **STATUTORY SCRUTINY ITEMS**

Crime and Disorder Issues

6.1 Retail Crime Investigation – Initial Evidence - *Statutory Scrutiny Manager*

Health Scrutiny Issues

6.2 Draft Joint Local Health and Wellbeing Strategy (2025-2030) – *Director of Public Health*

7. OTHER ITEMS FOR DECISION

7.1 Regulation of Investigatory Powers Act 2000 (RIPA) Annual Report (including Quarters 1 and 2 Update) – *Director of Legal, Governance and Human Resources*

7.2 Appointment Independent Persons Recruitment – *Director of Legal, Governance and Human Resources*

8. MINUTES FROM RECENT MEETINGS FOR RECIEPT BY THE COMMITTEE

8.1 Health and Wellbeing Board – None

8.2 Finance and Policy Committee relating to Public Health issues – None

8.3 Tees Valley Health Scrutiny Joint Committee – 15th March 2024

8.4 Safer Hartlepool Partnership – None

8.5 Tees Valley Area Integrated Care Partnership – None

8.6 Regional Health Scrutiny – None

8.7 Durham, Darlington and Teesside, Hambleton, Richmondshire and Whitby STP Joint Health Scrutiny Committee - None

9. ANY OTHER BUSINESS WHICH THE CHAIR CONSIDERS URGENT

For information: - forthcoming meeting dates: -

Tuesday 5 November, 2024 at 5.00 pm
Tuesday 10 December, 2024 at 5.00 pm
Tuesday 28 January, 2025 at 5.00 pm
Tuesday 4 March, 2025 at 5.00 pm
Tuesday 1 April, 2025 at 5.00 pm

AUDIT AND GOVERNANCE COMMITTEE

15th October 2024

Report of: Statutory Scrutiny Manager

Subject: RETAIL CRIME INVESTIGATION – INITIAL EVIDENCE

---

1. COUNCIL PLAN PRIORITY

Hartlepool will be a place*:
where people will be safe and protected from harm.
with a Council that is ambitious, fit for purpose and reflects the diversity of its community.

2. PURPOSE OF REPORT

2.1 To introduce baseline evidence as part of the initial stages of the Committee's Retail Crime investigation.

3. BACKGROUND INFORMATION

3.1 The Audit and Governance Committee at its meeting on the 24th September 2024 concluded the process for identification of its 2024/25 work programme. The Committee explored several potential topics for investigation, from across its scrutiny remit (including health and crime and disorder issues) and, with due regard to ensuring the most effective use of time and resources, agreed to focus on one in-depth investigation during 2024/25. It was agreed that an investigation of 'Retail Crime in Hartlepool' would be undertaken, providing a significant opportunity for partnership working with Cleveland Police (including support for ongoing prevention and detection activities).

3.2 It was agreed that:

- The **aim** of the investigation would be to 'look at ways of designing out and reducing incidents of retail crime'

- The **Terms of Reference** for the investigation would be:

  (a) To gain an understanding of the issue and its impact on residents, employees and businesses;

(b) To explore the factors that drive retail crime (national and local data inc. police information in relation to high level offenders);

(c) To examine existing approaches used to tackle the issue and investigate their effectiveness (preventative and reactive). E.g.

i) Are we encouraging retailers to maximise the use of new technologies for the prevention and detection of retail crime, including the facilitation of digital CCTV evidence?
ii) Are we encouraging Community Safety Partnership to direct investment to design out crime to areas they perceive to be a problem, including reducing opportunities to sell stolen goods?
iii) Are we actively encouraging the use of appropriate funding to invest in local retailers?
iv) Are there sufficient support pathways for those who use retail theft to fund substance misuse?
v) Are there sufficient food banks, advertised, accessible and with ongoing funding for those who use retail theft as a means during the cost of living crisis?
vi) Are there sufficient out of court resolution pathways available to residents of Hartlepool?

(d) To seek views on the issue, the impact and what could / should be done from:

- Residents (survey – as part of Police Ward surveys),
- Stakeholders and businesses (HBC survey and face to face Working Gorup)

(e) To gain an understanding of the impact of current and future budget pressures on the way in which services are provided.

(f) To identify potential ways of designing out and reducing incidents of retail crime.

- The **timetable** for the investigation:

15th October 2024

- To gain an understanding of the issue from a police perspective.
- Agree a process to seek the views of residents, stakeholders and businesses on the issue and what could / should be done to tackle it (survey / face to face session / potential working group)

5th November 2024

- Views / input from the Member of Parliament for Hartlepool (also Chair of the Safer Hartlepool Partnership), Cleveland Police, Police and Crime Commissioner and Chair of Neighbourhood services Committee.

- Exploration of the factors that drive retail crime

(date tbc) December - Working Group with businesses / stakeholders to discuss the issue, their experiences (experiences of staff) and what could / should be done to respond to it.

10th December 2024

- To examine existing approaches used to tackle the issue and investigate their effectiveness (preventative and reactive). E.g.

  i) Potential ways of designing out and reducing incidents of retail crime.
  ii) Are we encouraging retailers to maximise the use of new technologies for the prevention and detection of retail crime, including the facilitation of digital CCTV evidence?
  iii) Are we encouraging Community Safety Partnership to direct investment to design out crime to areas they perceive to be a problem, including reducing opportunities to sell stolen goods?
  iv) Are we actively encouraging the use of appropriate funding to invest in local retailers?
  v) Are there sufficient support pathways for those who use retail theft to fund substance misuse?
  vi) Are there sufficient food banks, advertised, accessible and with ongoing funding for those use retail theft as a means during the cost of living crisis?
  vii) Are there sufficient out of court resolution pathways available to residents of Hartlepool?

28th January 2024

- Further exploration of the factors that drive retail crime (offender lived experience evidence).
- Feedback from surveys / views of residents, stakeholders and businesses on the issue and what could / should be done to tackle it.
- To gain an understanding of the impact of current and future budget pressures on the way in which services are provided.

(Date TBC) February – Working Group to discuss formulation of recommendations

4th March 2024 – Approval of Final report by the Audit and Governance Committee

4. PRESENTATION OF EVIDENCE

4.1 As part of the first evidence gathering session, Chief Inspector Peter Littlewood will be present to provide the Committee with an overview of retail crime in Hartlepool from a police perspective. This will include an interactive question and answer session.

4.2 Work is ongoing to finalise proposals consultation and engagements as part of the investigation, including via Police Ward Surveys (residents), HBC engagement platform (businesses and stakeholder organisations) and face to face engagement with businesses. Details of the proposed engagement plan will be presented to the Committee at its meeting on the 15th October 2024.

5. RECOMMENDATION

5.1 That the Committee receive the information provided, as part of the first stage of the investigation, and consider the proposed consultation and engagement plan to be presented at the meeting.

Contact Officer: - Joan Stevens
Statutory Scrutiny Manager
joan.stevens@darlington.gov.uk
01429 284142

BACKGROUND PAPERS

The following background paper(s) was/were used in the preparation of this report:-

- Presentation by Superintendent Hopps at the Audit and Governance Committee Meeting on 16th July 2024
- Report and minutes of the A&G meeting held on the 16th July 2024 and 24th September 2024.

The above items can be viewed at Agendas, reports and minutes | Hartlepool Borough Council

AUDIT AND GOVERNANCE COMMITTEE

15 October 2024

Report of: Director of Public Health

Subject: DRAFT JOINT LOCAL HEALTH AND WELLBEING STRATEGY (2025-2030)

---

1. COUNCIL PLAN PRIORITY

Hartlepool will be a place:
- where people are enabled to live healthy, independent and prosperous lives.
- where those who are vulnerable will be safe and protected from harm.
- of resilient and resourceful communities with opportunities for all.
- that is sustainable, clean, safe and green.
- that has an inclusive and growing economy.
- with a Council that is ambitious, fit for purpose and reflects the diversity of its community.

2. PURPOSE OF REPORT

2.1 The purpose of this report is to present to the Audit and Governance Committee the final draft of the Joint Local Health and Wellbeing Strategy (JLHWS) for comment.

3. BACKGROUND

3.1 The Health and Social Care Act 2012 requires the Local Authority, with partner agencies including the NHS, to develop a JHWS based on the Joint Strategic Needs Assessment (JSNA). The Health and Care Act 2022 amended Section 116A of the Local Government and Public Involvement in Health Act 2007 and renamed 'joint health and wellbeing strategies' to 'joint local health and wellbeing strategies' (JLHWSs).

3.2 Health and Wellbeing Boards continued to be responsible for the development of joint strategic needs assessments (JSNA) and JLHWS. They are also responsible for deciding when to update or refresh JLHWSs or undertake a fresh process to ensure that they are able to inform local commissioning plans over time.

3.3 Hartlepool's JLHWS (2018-2025) was developed in 2017-2018 and the deadline for its refresh is March 2025. The decision was made by the HWB, on the 5 September 2022, for the Public Health Team to lead the refresh of the current 2018-2025 strategy. As part of the process, a stocktake of the previous strategy was undertaken in 2022/23 followed by a consultation, to inform the strategies priorities. The consultation incorporated into the councils 'Big Conversation' consultation (December 2023 - January 2024).

4. PROPOSALS

4.1 The results of these consultations have now been incorporated in to the final draft of the JHWS and we are now in a position to develop a JLHWS, that will inform the development of a detailed action plan and outcome framework which will be the responsibility of the HWBB to oversee and monitor. The strategy setting out the below priorities, for the next five years:

- **Starting Well** – All Children and young people living in Hartlepool have the best start in life.
- **Live well** - People live and work in connected, prosperous and sustainable Communities.
- **Age well** - People live healthier and more independent lives, for longer

4.2 A copy of the draft JLHWS is attached at **Appendix A**.

4.3 In accordance with the process contained within the Council's Constitution, the Audit and Governance Committee, as the Council's statutory scrutiny body, has a key role in the development of Budget and Policy Framework documents. Whilst the JLHWS is no longer a budget and policy framework document, as part of the final stage of the process for development and approval of the strategy, as detailed in Table 1 below, the Audit and Governance Committee is requested to comment on the draft version of the Hartlepool JLHWS. The views of the committee to be reported to the Health and Wellbeing Board for consideration during approval of the strategy, prior to its adoption by the Finance and Policy Committee on the 20 January 2025.

Table 1 - Process for Approval / Adoption of the Joint Local Health and Wellbeing Strategy

Where	Description	Date of Meeting
Health & Wellbeing Board	Review of Health & Wellbeing Strategy agreed	8 July 2024
Consultation activity / research and develop draft strategy (inc. Big Conversation results)		July / August 2024
Health & Wellbeing Board	Draft strategy approved for consultation	9th Sept 2024
Audit & Governance Committee	8 weeks consultation (Oct – Nov) - 6 week inc. A&G Statutory Scrutiny Elected Members / Public and Other Activities	15th Oct 2024
Finance & Policy Committee		25th Nov 2024
Consider consultation feedback & amend/redraft		25th Nov – 2nd Dec

strategy		2024
Health & Wellbeing Board	Final draft strategy considered by H&WB and F&P *(approve Strategy as the body responsible)*	2nd Dec 2024
Finance & Policy Committee	*(Adopt the strategy)*	20th Jan 2025

4.4 It is recognised that responsibility for the monitoring of the implementation of the JHWS sits within the remit of the HWB. However, given the Committee role as the Council's statutory health scrutiny body, Members are asked to consider it they feel it would be beneficial to receive an update report on the implementation of the strategy on a regular basis.

5. RISK IMPLICATIONS

5.1 The main risk is that the strategy is not refreshed within the timescales - it is a requirement of the HWBB to publish their Joint Health and Wellbeing Strategy setting out their priorities

6. OTHER CONSIDERATIONS

FINANCIAL CONSIDERATIONS	**None**
LEGAL CONSIDERATIONS	**None**
EQUALITY AND DIVERSITY CONSIDERATIONS	**None**
STAFF CONSIDERATIONS	**None**
ASSET MANAGEMENT CONSIDERATIONS	**None**
ENVIRONMENT, SUSTAINABILITY AND CLIMATE CHANGE CONSIDERATIONS	**This will be developed alongside the strategy.**

7. RECOMMENDATIONS

7.1 That the Audit and Governance Committee:

i) Consider the draft version of the Hartlepool JLHWS (2025-2030) and express any view it wishes relaying to the Health and Wellbeing Board, to assist in its consideration of approval of the strategy;

ii) Agree that an update report in relation to the implementation of the JLHWS (2025-2030) will be submitted for Members consideration on an annual basis.

8. BACKGROUND PAPERS

Agenda and Minutes:
- Health and Wellbeing Board (8 July 2024 and 9 September 2024)

- Audit and Governance Committee (15 October 2024)

Acts:
- Health and Social Care Act 2012
- The Health and Care Act 2022
- Local Government and Public Involvement in Health Act 2007 (Section 116A)

9. CONTACT OFFICERS

Craig Blundred
Director of Public Health
Email: Craig.Blundred@hartlepool.gov.uk

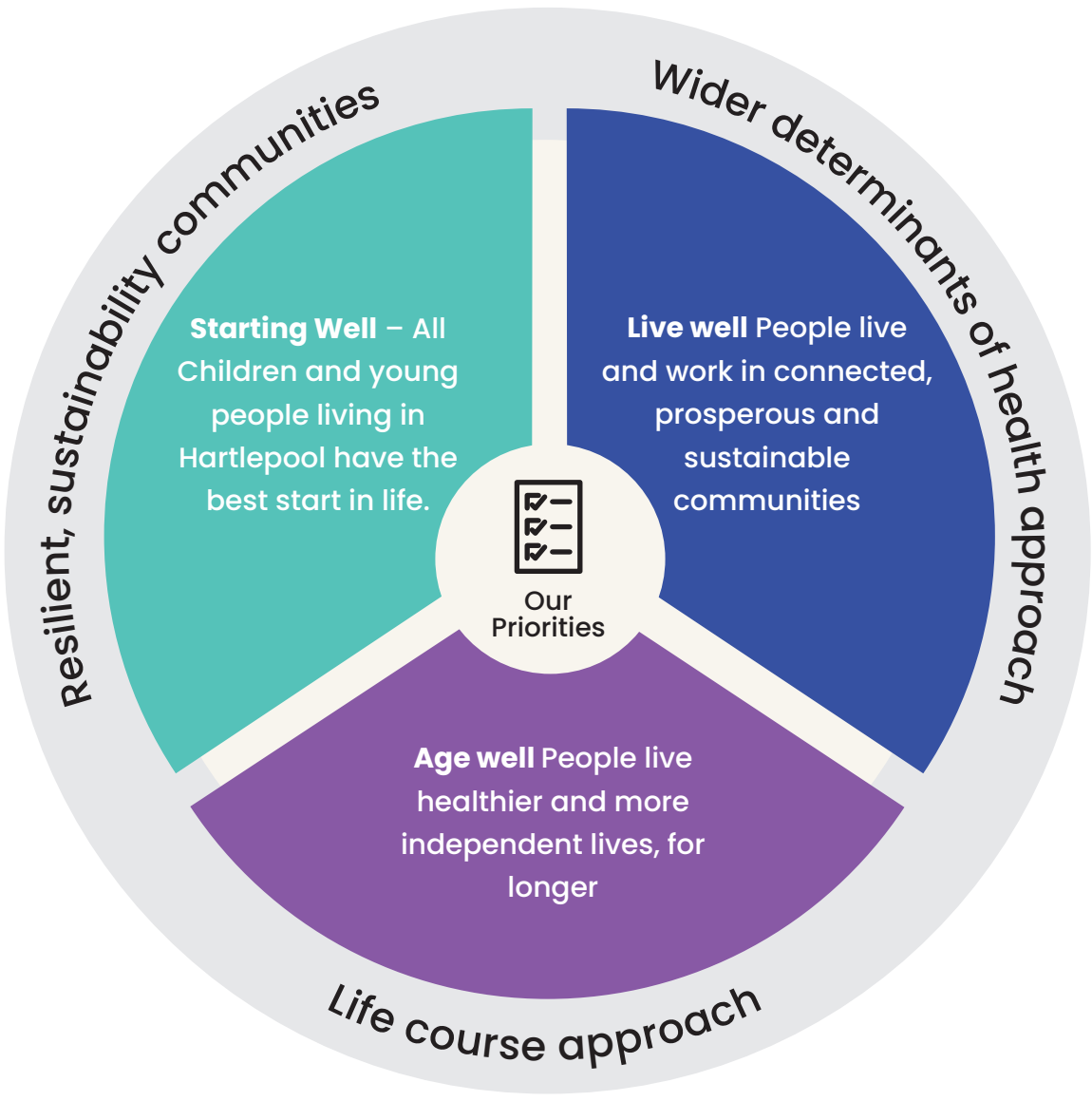
Claire Robinson
Public Health Principal
Email: Claire.Robinson@hartlepool.gov.uk

Joint Health and Wellbeing Strategy on a page

Our Vision: We will address health inequalities by working together to ensure everyone in Hartlepool has the opportunity to thrive and achieve their potential

Principles

- Tackling inequalities
- Empowering local communities
- Shared responsibility
- Integrated approaches
- Building Health



The Board will develop an action plan which measures identified priority areas against the principles and priority themes.

AUDIT AND GOVERNANCE COMMITTEE

15 October 2024

Report of: Director of Legal, Governance and Human Resources

Subject: REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) ANNUAL REPORT (INCLUDING QUARTERS 1 AND 2 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 2000.

2. BACKGROUND

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 OF RIPA

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 2023/2024:-

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

4.2 In the quarters to the date of this meeting:

Quarter 1

Communications Data	Nil
CHIS	Nil
Directed Surveillance	Nil

Non –RIPA	Nil
External	Nil

Quarter 2

Communications Data	Nil
CHIS	Nil
Directed Surveillance	Nil
Non –RIPA	Nil
External	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 has been to reflect changes in job titles of senior Officers.

6. ACTIVITY IN THE CURRENT YEAR

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

6.3 Arrangements are being made for Officer RIPA Training and Awareness which will take place in November 2024. This will be attended by a number of Officers from a range of Departments across the Authority.

6.4 Awareness of RIPA to continue to be raised across the Council. An e mail has been sent to all staff reminding them of 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 in the RIPA policy.

6.5 Information continues to be made available on the RIPA pages of the Council's intranet and internet.

7. INSPECTIONS

7.1 The Authority received a request from IPCO regarding a 'desktop' examination (previous inspection had been in 2021).

7.2 Elected Members are advised that the outcome of the inspection was that the Investigatory Powers Commissioner was assured of ongoing compliance with RIPA 2000 and that the Investigatory Powers Act 2016 will be maintained. As such, further inspection was not required this year.

7.3 The Inspector highlighted, however, that in relation to the one authorisation granted in the past three years, there had been a number of points:

- The dates that the applicant and the Authorising Officer had indicated as having completed their inputs were incorrect; being cited as January 2021 when they were in fact January 2022. This was acknowledged as typing error.
- The application for judicial approval and subsequent approval should have been on the national template forms by the applicant and magistrate respectively. These forms are included as Annex B in the '*Home Office Guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice'*. This issue has been highlighted to appropriate Officers who have been requested to remind Magistrates of the national template forms.
- The actual surveillance activity achieved its objectives but there was a failure to cancel the authorisation. Authorisations should always be cancelled, rather than just being allowed to 'whither on the vine'. Officers have been reminded of cancellation requirements. Procedure Note has also been updated accordingly.

7.4 The Inspector noted a Non-RIPA authorisation which had been granted in November 2022. This had been an overarching authorisation that authorised staff to use social media for any subsequent case or investigation relating to child safeguarding. Whilst recognised as laudable to seek some form of approval for this generic information gathering tool, the Inspector had mentioned that it is more appropriate for such activity, that does not reach the criteria for authorisation as directed surveillance, to perhaps be authorised a generic authorisation but that should be supplemented by an auditable record of what activity is carried out on a case by case basis and many local authorities have such processes in place. This audit trail does not need to be too onerous but sufficient to show what took place and the reason why. The Director of Legal, Governance and Human Resources undertook to query with other local authorities in the region to see if such a process was being used. In the meantime, the Executive Director, Children's and Joint Commissioning Services was consulted and advised that she would expect that case by case activity would be recorded in a child's record where this was used.

7.5 The Inspector was informed of the responses included above and responded that 'the response is both prompt and appropriate'.

8. SURVEILLANCE POLICY

8.1 The Council's RIPA Policy is available on the Council's intranet and is appended to this report **(Appendix A)**. A finding from the 'desktop' inspection was that the Policy and Procedure document required some slight amendment at paragraph 6.9.1 where it was stated that if a Juvenile is authorised as CHIS this lasts for one month rather than the correct period of four months.

8.2 Following the retirement of the Legal and Democratic Services Team Manager in June 2024, the Policy was updated to reflect the new RIPA co-ordinator, Leanne Purdy.

9 RECOMMENDATIONS

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

10. REASONS FOR RECOMMENDATIONS

10.1 To enable the Council to operate the RIPA system effectively and as required by law and guidance.

10.2 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.

11. CONTACT OFFICER

11.1 Hayley Martin
Director of Legal, Governance and Human Resources and Senior Responsible Officer for RIPA
Hayley.martin@hartlepool.gov.uk
01429 523003

12. 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	Director of Legal Governance and HR
Version	5
Issue date	September 2024
Approved by	Director of Legal Governance and HR
Next Revision Due	September 2025

INDEX

APPENDICES

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 directed surveillance or CHIS 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 Investigatory Powers 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 Director of Legal Governance and HR

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

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
- Executive Director of Development, Neighbourhoods and Regulatory Services
- Senior Responsible Officer (in the absence of the above)

3.2.4 For authorisations 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 Officer (Information & Litigation) 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 sought and granted by another authority	Quarterly Report Annual report

Review of the effectiveness of this policy and any recommendation for changes to be made	Annual Report – with any significant Amendments referred to Council for approval.

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 Director of Legal Governance and HR.

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 <u>Social Networking Sites (SNS)</u>

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 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 21 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 4 months 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 b e 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 Director of Legal Governance and HR 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/a

ttachment_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

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

Yes / No

- Complete RIPA authorisation/ notice form, and seek approval of authorising officer/designated person as per current arrangements.
- Complete application part of the judicial application/order form for JP.

Within Office Hours

Local authority investigator (or an appointed representative of the Legal Division) to contact Her Majesty's Courts & Tribunals Service (HMCTS) court to arrange a hearing.

Outside usual office hours:

A JP may consider an authorisation out of hours in **exceptional** circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:

- Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
- If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
- Attend hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.

s the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

No / Yes

Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
-Section 7 of the Children and Young Persons Act 1993.

No / Yes

Local authority investigator (and/or an appointed representative of the Legal Division) attend court with:

- counter-signed RIPA authorisation/ or notice (for CD authorisations/ notices the signatures may be electronic signatures).
- the accompanying judicial application/order form.

Outcome

Investigator **may not** use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met If further offences come to light as the case progresses.

Refuse to approve the grant or renewal and quash the authorisation or notice.

Refuse to approve the grant or re-newal of an authorisation or notice.

Approve the grant or re-newal of an authorisation or notice.

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.

The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may **not** use the covert technique. Local authority may wish to address, for example, a technical error and reapply.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

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.

HARTLEPOOL BOROUGH COUNCIL

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 Leanne Purdy, 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:

4. Describe the purpose of the surveillance.

5. 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:

6. The identities, where know, 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 why surveillance is NECESSARY in this particular case:

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

8. Explain why 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

15 October 2024

Report of: Director of Legal, Governance and Human Resources

Subject: APPOINTMENT INDEPENDENT PERSONS RECRUITMENT

---

1. PURPOSE OF REPORT

1.1 The Committee's approval is sought to make arrangements for the recruitment and selection of up to three Independent Persons whose appointment must then be approved by a majority of Elected Members at Full Council.

1.2 The report serves as a reminder of the requirement for, and the role of, the Independent Persons and provides a suggested recruitment and selection process to be carried out to enable the Authority to make appointments at the start of the 2025/26 Municipal year.

2. BACKGROUND

2.1 The Committee is aware that Sections 28(7) to (10) of the Localism Act 2011 require the Council to appoint at least one "Independent Person" – essentially not a current Officer, Member or Co-opted Member of the Council, or a person who has been an Officer, Member or Co-opted Member of the Council within the past 5 years, or a relative or close friend of either of the aforementioned categories. The Localism Act provides that the views of an Independent Person must "be sought, and taken into account" by the Council "before it makes a decision on an allegation that it has decided to investigate". In addition the Localism Act provides that the views of an Independent Person may be sought by the Council when deciding how to deal with a new allegation.

2.2 More recently the Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015 introduced an additional formal statutory role for Independent Persons, requiring them to work together as a Panel in advising the Council prior to any vote on whether to dismiss the Council's Head of Paid Service, Monitoring Officer and Chief Finance Officer, ('Protected Officers'). Under these regulations, the Independent

Advisory Panel must contain at least two Independent Persons. The Redmond Review into the Oversight of Local Audit and the Transparency of Local Authority Financial Reporting recommends consideration being given to the appointment of at least one suitably qualified independent member, to the Audit Committee.

3. PROPOSALS/ISSUES FOR CONSIDERATION

3.1 Since 2013 the current and former Monitoring Officers have worked effectively and efficiently with the Independent Persons appointed by Council in accordance with the requirements of the Localism Act. To date there has been no requirement for them to advise Council in relation to the dismissal of Protected Officers.

3.2 Previously the Council appointed two Independent Persons in 2023, however following the resignation of Tracy Squires, we are currently operating with one, namely Martin Slimings whose term of office is due to end in May 2025. Audit and Governance Committee's approval is sought to enable the Monitoring Officer to make the appropriate arrangements for the recruitment and selection of up to three Independent Persons with a term of office commencing in May 2025. As part of this process, Martin Slimings will have the opportunity to apply to renew his current appointment. In order to comply with the Redmond Review it is suggested if possible, one of the three Independent Persons have relevant financial experience in order to strengthen transparency and accountability.

3.3 The recruitment pack to be utilised for this purpose is attached at Appendix 1 and Members' views are sought. In line with ongoing Government consultation it is suggested that the Independent Persons appointment be for a term of office of 2 years. It is hoped that the timetable can be undertaken to enable the Independent Persons to take up their role from May 2025.

3.4 It is suggested that the vacancies be advertised on social media and in local newspapers and on the Council website. A shortlisting exercise and subsequent interview panel will then be conducted by the Chair and Vice Chair of the Audit and Governance Committee with the Director of Legal, Governance and Human Resources and Monitoring Officer and Executive Director of Development, Neighbourhoods and Regulatory Services.

The Panel's proposals will be presented to Council in May 2025 for approval.

4. RECOMMENDATIONS

4.1 That the Audit and Governance Committee approve the recruitment process for up to three Independent Persons to undertake the role as provided in Appendix 1.

5. REASONS FOR RECOMMENDATIONS

5.1 To ensure the Council complies with Sections 28(7) to (10) of the Localism Act 2011 along with the Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015.

6. BACKGROUND PAPERS

Localism Act 2011
Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015
Redmond Review into the Oversight of Local Audit and the Transparency of Local Authority Financial Reporting

7. CONTACT OFFICER

Hayley Martin
Director of Legal, Governance and Human Resources
Hartlepool Borough Council
Civic Centre
Hartlepool, TS24 8AY

Tel: 01429 523003

RECRUITMENT PACK FOR

APPOINTMENT OF

INDEPENDENT PERSONS

APPENDIX 1

HARTLEPOOL BOROUGH COUNCIL

APPOINTMENT OF INDEPENDENT PERSONS

TO THE AUDIT AND GOVERNANCE COMMITTEE AND INDEPENDENT ADVISORY COMMITTEE

Under the Localism Act, 2011, the Borough Council are required to appoint at least one Independent Person as part of their arrangements in the promotion and maintenance of high standards of conduct affecting its Elected Members and those members of a Parish Council within its area.

In addition, the Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015 provides an additional formal statutory role for Independent Persons, requiring them to work together as an Independent Advisory Panel in advising the Council prior to any vote on whether to dismiss the Council's Head of Paid Service, Monitoring Officer and Chief Finance Officer, ('Protected Officers'). Under these regulations, the advisory Panel must contain at least two Independent Persons.

Applications are therefore invited from members of the public to undertake the role of Independent Persons (term of office two years) as noted above, particularly from those with experience in either a regulatory, commercial, financial, professional or voluntary sector with an interest in the proper and effective ethical and good governance of an organisation.

Training will be provided and reasonable travel and subsistence expenses will be payable.

Applicants should not within the past five years have been an Elected Member, Co-Opted Member or Officer of the Borough Council or of a Parish Council within the Council's area, or a relative or close friend of such persons.

An application pack, including application form and role description is available upon request. For an informal discussion about these posts please contact Hayley Martin, Director of Legal, Governance and Human Resources, Hartlepool Borough Council on 01429 523003.

Completed applications should be returned to:

Gemma Jones
Scrutiny and Legal Support Officer
Hartlepool Borough Council
Civic Centre
Victoria Road
Hartlepool
TS24 8AY

Gemma.Jones@hartlepool.gov.uk

APPENDIX 1

INDEPENDENT PERSON ON THE AUDIT AND GOVERNANCE COMMITTEE, INDEPENDENT ADVISORY COMMITTEE SELECTION CRITERIA

SKILLS AND COMPETENCIES

The Independent Person will have:

- a keen interest in standards in public life.
- a wish to serve the local community and uphold local democracy.
- the ability to be objective, independent and impartial.
- sound decision making skills.
- leadership qualities, particularly in respect of exercising sound judgement.

The Independent Person will:

- be a person in whose impartiality and integrity the public can have confidence.
- understand and comply with confidentiality requirements.
- have a demonstrable interest in local issues.
- have an awareness of the importance of ethical behaviours.
- be a good communicator.

Desirable additional criteria are:

- working knowledge/experience of local government or other public service and/or of large complex organisations and awareness of and sensitivity to the political process.
- knowledge and understanding of judicial/quasi-judicial, complaints and audit processes.
- relevant financial knowledge/experience in either the public or private sector that would aid the understanding and review of financial and audit reports.
-

You should demonstrate in your application how you meet the above criteria as this will assist any short-listing process.

Means of assessment will be by application form and by interview.

NOTE: You will be required to be contactable at all times during normal working hours by telephone or by email and to be available to attend hearings which may be held in the day time and at relatively short notice.

Eligibility for Appointment

A person cannot be appointed as an Independent Person if they are actively engaged in local party political activity in any way or, if they are or were within a period of 5 years prior to the appointment:

- An Elected Member, co-opted member or officer of the Authority.
- An Elected Member, co-opted member or officer of a parish council in the Borough Council's area, or a relative or close friend of the above.

APPENDIX 1

ROLE OF INDEPENDENT PERSON

ROLE DESCRIPTION

Responsible to: The Council

Liaison with: Monitoring Officer, Members of the Audit and Governance Committee, Executive Director of Development, Neighbourhoods and Regulatory Services, Officers and Members of the Council, and parish councillors within the Borough, key stakeholders within the community.

1. To assist the Council in promoting high standards of conduct by Elected and Co-opted Members of the Council and parish councillors and in particular to uphold the Code of Conduct adopted by the Council including the principles of public office, namely; selflessness, honesty, integrity, objectivity, accountability, openness and leadership.

2. To review and approve the work of the Authority's internal auditors and review the plans of the external auditor and the internal audit team to ensure that Audit work is co-ordinated. Ensure adequate corporate governance arrangements in respect of risk management and fraud prevention are in place and operate effectively.

3. To be consulted by the Council through the Monitoring Officer and/or the Audit and Governance Committee before it makes a decision on an investigated allegation and to be available to attend meetings of the Hearing Sub-Committee of the Audit and Governance Committee for this purpose.

4. To be available for consultation by the Monitoring Officer and/or the Audit and Governance Committee before a decision is taken as to whether to investigate a complaint or to seek local resolution of the same.

5. To be available for consultation by any Elected Member, including parish councillors who is the subject of a complaint.

6. To develop a sound understanding of the ethical framework as it operates within the Council and Parish Councils within the Borough.

7. To participate in an Independent Advisory Committee to provide advice to the Council prior to any vote on whether to dismiss the Council's Head of Paid Service, Monitoring Officer and Chief Finance Officer, ('Protected Officers').

8. To participate in training events to develop skills, knowledge and experience and in networks developed for Independent Persons.

9. To attend training events organised and promoted by the Council.

10. To act as advocate and ambassador for the Council in promoting ethical behaviour.

EXTRACT

COUNCIL'S CODE OF CONDUCT

APPENDIX 1

APPLICATION FOR THE POSITION OF INDEPENDENT PERSON

Individuals who wish to be considered for appointment as Independent Person are requested to provide the following information to support their application. All information provided will be treated in the strictest confidence and will only be used for the purposes of selection. Please feel free to use a separate continuation page if you wish to expand upon your answer to any question outlined below.

1. PERSONAL DETAILS

Name:

Address:

Postcode:

National Insurance Number:

Contact Details:

Daytime Telephone Number:

Email Address:

2. QUALIFICATIONS
(Please list in particular any qualifications which you think are relevant to these roles)

3. SUMMARY OF EXPERIENCE
(Please give a brief account of your experience including career, public and voluntary work together with the nature of your current or most recent occupation)

4. RELEVANT EXPERTISE/SKILLS
(Please outline briefly any knowledge or expertise which you believe would be particularly relevant having regard to the selection criteria and role descriptions)

5. Why do you wish to be considered for appointment and what particular attributes do you believe you would bring to these roles?

6. Please provide any additional information you may wish to give in support of your application:

7. <u>References will be taken up for all applicants who are invited for interview</u>

1. Name:	2. Name:
.....	.....
Address:	Address:
.....	.....
.....	.....
.....	.....
.....	.....
Telephone No.	Telephone No. .....

I wish to apply to be an Independent Person.

In submitting this application, I declare that:

<u>EITHER</u>

- I am not and have not during the past five years been an Elected Member or Officer of the Borough Council.
- I am not related to, or a close friend of, any Elected Member or Officer of the Borough Council.
- I am not currently an Officer or Elected Member of any other relevant authority (this includes parish, unitary councils and Police and Fire Authorities).
- I am not actively engaged in local party political activity.

Signed: .....

Date: .....

Please return this application form marked **<u>PRIVATE AND CONFIDENTIAL</u>** and addressed to:

Gemma Jones
Scrutiny and Legal Support Officer
Hartlepool Borough Council
Civic Centre
Victoria Road
Hartlepool
TS24 8AY

Or email the completed form to Gemma.Jones@hartlepool.gov.uk

Tees Valley Joint Health Scrutiny Committee

A meeting of the Tees Valley Joint Health Scrutiny Committee was held on Friday 15 March 2024.

Present: Cllr Marc Besford (SBC) (Chair), Cllr Rachel Creevy (HBC) (Vice-Chair), Cllr Ceri Cawley (R&CBC), Cllr Lynn Hall (SBC), Cllr Mary Layton (DBC), Cllr Paul McInnes (R&CBC), Cllr Vera Rider (R&CBC), Cllr Jan Ryles (MC), Cllr Susan Scott (SBC)

Officers: Michael Conway (DBC); Gemma Jones (HBC); Sarah Connolly (R&CBC); Gary Woods (SBC)

Also in attendance: Dan Jackson (North East and North Cumbria Integrated Care Board); Dominic Gardner, Chris Morton, Beverley Murphy (Tees, Esk and Wear Valleys NHS Foundation Trust); Mark Cotton (North East Ambulance Service NHS Foundation Trust)

Apologies: Cllr Jonathan Brash (HBC), Cllr Christine Cooper (MC), Cllr Brian Cowie (HBC), Cllr Heather Scott (DBC), Cllr Jeanette Walker (MC)

1	**Evacuation Procedure** The evacuation procedure was noted.
2	**Declarations of Interest** There were no interests declared.
3	**Minutes of the Meeting held on 15 December 2023** Consideration was given to the minutes from the Committee meeting held on 15 December 2023. Attention was drawn to the following item that was on the agenda: • Office for Health Improvement & Disparities - Community Water Fluoridation: Clarity was sought on what was agreed at the conclusion of this item, with some Members commenting that they were only in support of the planned consultation process, not necessarily the proposals to expand community

	water fluoridation in the North East of England. Following a brief debate (which included the noting of some new related information that some Members had received from an anti-fluoride group, an entity which, according to other Members, had been previously discredited), it was agreed to amend the minutes to reflect that the Committee agreed to support the consultation process only. AGREED that the minutes of the Committee meeting on 15 December 2023, subject to the identified amendment for the 'Office for Health Improvement & Disparities - Community Water Fluoridation' item be approved as a correct record.
4	**North East and North Cumbria Integrated Care Board - Update on Recent Restructure** The Committee received an update following the recent restructuring of North East and North Cumbria Integrated Care Board (NENC ICB). Led by the NENC ICB Director of Policy, Involvement and Stakeholder Affairs, content included: ➢ ICB 2.0 Organisational Restructure: A new way of working ➢ Significant change ➢ Executive team ➢ The NENC way ➢ Local Delivery Team comparison ➢ Contracting and devolution of budgets ➢ Networks and workstreams ➢ Example - Clinical Networks and ODNs ➢ Initial work - Networks and Alliances ➢ Still work to do… The Committee was informed that the NHS typically went through a period of restructure approximately every decade. However, the formal implementation of the new national Integrated Care System (ICS) less than two years ago (mid-2022) already involved the merging of eight former Clinical Commissioning Groups (CCGs) into one regional organisation – the NENC ICB. In addition, from the onset of these new arrangements, further responsibilities were adopted and other subsequent delegations (i.e. pharmacy / optometry and dental in April 2023) had followed, with more anticipated in relation to specialist commissioning. Despite their relative infancy, ICBs had been instructed to reduce running costs by 30%, a task the NENC ICB was still working through (though around 100 posts had already been lost) – this exercise involved collaboration with each of the 14 Local Authority areas within the NENC footprint, reflecting the ICBs 'place-based' working approach. Moving forward, several key elements would underpin 'the NENC way' – these included a clinically-led (multi-disciplinary) and managerially-enabled focus, a structure involving eight directorates with eight executive directors, and enabling and delivery teams (the latter seeing six teams mapped to the 14 Local Authority partners, one of which would be 'Tees Valley' (comprising five Local Authorities))

	concentrated on the delivering the vision and constitutional standards. Local committees mapped to each Local Authority area would continue. Networks and workstreams were charted, with some inherited, some developing, and all at different levels of maturity. Clinical networks were either managed by NHS England or were transitioning to the ICB. Operational Delivery Networks (ODNs), managed within acute provider organisations but accountable to NHS England, outlined how pathways needed to work – these were listed along with the NENC clinical networks. Regarding the latter, thematic groupings / alliances were being developed to give a better strategic view of specific health conditions. In terms of work still to do, it was expected that the mapping of system, clinical, corporate and operational delivery networks and workstreams would conclude by April 2024, and that a set of recommendations would then be created which contributed towards a streamlined organisation (reducing duplication), ensured work was aligned to the NENC ICBs *Better Health and Wellbeing for All* strategy, and enabled teams to deliver in accordance with a clear Terms of Reference. Clarity around funding and reporting mechanisms, as well as the provision of effective communication across the wider health and care system, was also envisaged. Thanking the NENC ICB representative for the presentation, the Committee immediately drew attention to the quoted loss of 100 posts (following the request to reduce running costs by 30%) and the potential for significant redundancy costs. In response, Members heard that the ICB inherited all CCG staff when it came into being, some of whom were permanent and others who were on a fixed-term contract. Opportunities to apply for voluntary redundancy / early retirement were offered, and assurance was given that there were no additional costs incurred in relation to this reduction in the workforce. It was noted that the vast majority of ICB expenditure was on its staffing resource. Referencing the 'Initial work – Networks and Alliances' slide, the Committee commented that a number of the nine categories appeared to have some form of crossover with other identified themes listed. Members were informed that the nine groupings merely represented initial thoughts, however, once confirmed, the work of these networks / alliances should benefit from a simpler decision-making process that a single ICB allowed (as opposed to the CCG era where strategic decision-making proved more challenging). The Committee highlighted instances of people across Tees Valley accessing services in North Yorkshire (e.g. Friarage Hospital, Northallerton) and were given subsequent assurance that collaborative arrangements with neighbouring ICBs were in place to address issues that arose. Members welcomed this, though also called for developments which may have an impact on the people of Tees Valley, wherever this may be, to be appropriately scrutinised (the former Durham, Tees Valley and North Yorkshire joint health scrutiny committee was referenced). AGREED that the North East and North Cumbria Integrated Care Board

	restructure information be noted.
5	**Tees, Esk and Wear Valleys NHS Foundation Trust - Quality Account 2023-2024** Representatives of Tees, Esk and Wear Valleys NHS Foundation Trust (TEWV) were in attendance to provide their annual presentation to the Committee in relation to the organisation's Quality Account, a document which NHS Trusts had a duty to produce each year. The TEWV Chief Nurse, supported by the TEWV Care Group Director MHSOP / AMH and the TEWV Lived Experience Director for Durham, Tees Valley and Forensics, covered the following elements: ➢ Quality Account Quality Priorities 2023/24 ➢ Priority 1: Care Planning ➢ Priority 2: Feeling Safe ➢ Priority 3: Embed the New Patient Safety Incident Response Framework (PSIRF) ➢ Setting the 2024/25 Quality Priorities ➢ Timeline Agreed by the TEWV Quality Assurance Committee in May 2023, the Trust's quality priorities for 2023-2024 were developed following discussion and review of quality data, risks and future innovations in collaboration with colleagues, patients, families and carers. Delivering on these priorities supported the ongoing mission to ensure that safe, quality care was at the heart of all TEWV did in line with its *Our Journey to Change* initiative and Quality Strategy. • <u>Priority 1: Care Planning</u>: The Trust had identified several aims for completion by 31 March 2024 involving new system developments, measurable goals within care plans, the publication of new policies and procedures, and data collection / monitoring mechanisms to assess the effectiveness of clinical interventions. Whilst it was stated that performance impact was not yet where the Trust would want it, progress during the year was then outlined, a key element of which was the delayed implementation of (and associated training on) the new CITO patient record system which went live on 5 February 2024. Other areas noted included the continuation of region-wide work with relevant stakeholders to move away from the Care Programme Approach (CPA) (the five principles signalling how systems should start to do this were subsequently listed), the now fortnightly meeting of the Personalising Care Planning Oversight Group to provide oversight and assurance to other workstreams / groups, and the continuation of the Care Planning Co-production Group which informed TEWV from a lived experience perspective. In related matters, six priorities for personalised care were highlighted – workforce (job descriptions), workforce (what is our offer?), data (e.g. waiting time metrics), interoperability (ICBs), managing risk and accountability, and working with partner organisations. Regarding the latter, it was noted that

TEWV was often one of a number of entities involved in an individual's care, therefore effective links with partners (including schools) was important. Understanding data around inequalities and how this may help identify different needs (and therefore service requirements) across various geographical areas was also emphasised. From a wider perspective, the seven NENC ICB priorities around care planning were also outlined.

- Priority 2: Feeling Safe: To ascertain a better understanding of why some patients did not feel safe on TEWVs wards, as well as what would help foster a greater sense of safety, the Trust engaged with individuals using its inpatient services. Feedback on both these elements was relayed, with common themes being a lack of / need for appropriate staffing levels, involvement in their own care, opportunities for meaningful activity, access to quiet areas, and support when unwell or when incidents had occurred within their environment. Crucially, reassurance from staff and staff support was a key protective factor in ensuring that patients felt safe on the ward, with patients stating that they valued their relationships with staff.

  It was explained that 'feeling safe' was not a mandated measure nationally and that all Trusts had different ways of determining and presenting this (hence benchmarking was not viable). Also emphasised was the possibility that not feeling safe could be an inherent feature of an individual's condition. To aid its aim of creating a positive relationship in which patients felt safe, TEWV had three key elements to achieve by the fourth quarter of 2023-2024 (January to March 2024), namely the implementation of the range of actions identified from the Feeling Safe Focus Groups with patients and staff, the continuation of the body-worn camera pilot work (and evaluation of impact), and the continued implementation of the *Safewards* initiative (an evidence-based model to support and enable patients to feel safe).

  Progress against these three areas of focus was documented, with dedicated Action Plans being produced and monitored for services where particular concerns had been identified by the Feeling Safe Focus Groups, and a process put in place to develop an overarching rationalised strategic workplan and reporting framework in relation to 'feeling safe' (specific work undertaken within Durham, Tees Valley and Forensics in response to the care group being given a performance improvement notice was also noted). Benefits and challenges associated with the body-worn camera pilot were highlighted (it was also acknowledged that this was a controversial topic, with some (including patients) liking this and others not), with an in-depth review of the pilot now a component of the Trust's Positive and Safe Plan (approved by the Quality Assurance Committee in August 2023). In terms of *Safewards*, the need to refocus the corporate approach to the implementation, monitoring, reporting and assessment of outcomes for these standards had been agreed.

  Developments in relation to TEWVs use of the question, '*During your stay, did you feel safe?*' were outlined. Following review by the Trust's Lived Experience Directors (with support from members of the Involvement Team), it

had been agreed that analysis would now reflect a two-answer configuration and include 'yes, always' and 'most of the time'. This change was made following the gathering of significant intelligence through focus groups which indicated that there were genuine reasons why people may not feel safe on an acute admissions ward.

Responding to a question on why Trusts were not mandated to track if people felt safe, the Committee was informed that, whilst this was a matter for NHS England, regulators would want to know if TEWV had mechanisms in place to ascertain how safe its service-users felt.

Linked to the first priority around care plan personalisation, the Committee asked if there was a way of establishing an agreed baseline measure with an individual where they can agree to feeling safe. A recent TEWV Board of Directors meeting involving a contribution from a care-experienced person who reflected on positive changes whilst using the Trust's services was referenced, and it was also noted that the new CITO patient record system should help support the co-production (between patients and clinicians) of safety plans.

Returning to the lack of a standardised national 'feeling safe' metric, the Committee expressed unease that TEWVs decision to change the way it presents feedback on its existing question could be interpreted as a means to merely achieve better-looking outcomes. Hartlepool Borough Council's health scrutiny function was writing to the NENC ICB with the aim of getting clarity around this situation and possibly establishing a baseline measure which could enable benchmarking, an endeavour the Committee agreed to support by sending its own correspondence.

The sensitive issue of body-worn camera use was probed, with Members asking if there had been any concerns raised around privacy. TEWV officers stated that employing such technology required careful consideration as there was the potential for misuse. The Trust drafted a policy for this some time ago (something the Lived Experience group had since examined), and, like the principles behind Oxehealth / OxeVision, its use had to be considered on an individual basis. If someone was not comfortable, both patient and staff needed to understand why.

The Committee drew attention to the '*How will we know we are making things better?*' table (included alongside the aims for completion by the fourth quarter of 2023-2024), and felt that the lack of change in the percentage of inpatients feeling safe / supported by staff to feel safe throughout 2023-2024 suggested the measures being used to address this quality priority (e.g. body-worn cameras) were not working. TEWV officers reiterated that the wrong question was being asked of people who may not feel safe under any circumstance, and that the Trust had perhaps not helped itself in using / publishing such a measure when other Trusts asked / reported on this in different ways. It was also highlighted that the previous year (2022-2023) had seen reduced occupancy within TEWV services (possibly as a result of the ongoing impact of the COVID-19 pandemic) which

meant staff had more time for patients compared to the 2023-2024 period. Like most Trusts, TEWV was experiencing challenges around demand for its services – this was linked to wider system pressures that were being caused by a number of factors (e.g. cost-of-living).

- Priority 3: Embed the New Patient Safety Incident Response Framework (PSIRF): By the fourth quarter of 2023-2024 (January – March 2024), TEWV aimed to achieve five elements within this priority, including compliance with the national PSIRF requirements, increasing staff completion of national Patient Safety Syllabus training (level 1 and 2), introducing an annual patient safety summit and the role of patient safety partners, and completing focused work on Duty of Candour through the delivery of an improvement plan.

  A summary of the implementation of PSIRF noted significant preparatory work undertaken over the past two years which ultimately led to the process going 'live' on 29 January 2024. A multi-disciplinary team (MDT) thematic review of serious incidents was undertaken in early-November 2023 and future quarterly reviews would be scheduled in collaboration with key specialty / directorate colleagues to review quarterly themes and to ensure learning was identified and embedded in workstreams and / or monitored.

  Other achievements were relayed in relation to Patient Safety Syllabus training (89% staff compliance for level 1; 66% for level 2), secured monies to fund two part-time Patient Safety Partner (PSP) posts (though a recent development meant this was now in doubt), and the ongoing delivery of the Duty of Candour improvement plan which would include a forthcoming independent audit to check progress. Once PSIRF was embedded, the annual Patient Safety Summit would be held.

The Committee asked if the Trust was meeting its deadlines with regards PSIRF. Assurance was given that these were being met and that this ensured that immediate learning was established.

The presentation concluded with details on the process for setting the TEWV quality priorities for 2024-2025 (the importance of these being co-created with service-users and carers was emphasised), and the remaining timeline for the consultation period and publication of the Trust's Quality Account 2023-2024 document.

Members probed the recruitment of Lived Experience staff, with TEWV highlighting the benefits of peer support and the important role of Lived Experience Forums within the community which allowed wider engagement and a potential pathway for future use of care-experienced individuals to help shape service delivery.

Whilst pleased that the Lived Experience work had become more established, the Committee commented that TEWV had been on its 'journey to change' for some time now and queried how far along it felt it was. In response, the anticipated

	benefits of the new CITO system were reiterated, the routine checking of whether carers were being identified and engaged / involved was highlighted, as was the mandated monthly Quality Board where TEWV had an agenda set for them. From a regulatory perspective, the last CQC inspection saw the Trust's three 'inadequate' domains improve, though it was acknowledged that the focus needed to be on patient safety (the historical backlog of serious incidents to report on were noted). Some staffing issues had also been identified, but these had since been addressed – Members felt it would have been helpful to have more detail on this latter statement, and also drew attention to the very limited statistics / data within the presentation, something which made it very difficult to determine performance / progress. Continuing the workforce theme, the Committee asked about the results of the recent staff survey. TEWV officers stated that this was a mandated survey, and that feedback was reflecting positive strides over the last year (data would be published nationally in the near future). Reflecting on the content of the presentation, Members felt there was little mention of 18-25-year-old provision and the challenges around transitioning from children's to adult services – assurance was given that development work was ongoing in relation to this demographic. In other matters, it was acknowledged that neurodiverse individuals had been poorly served for years, and that TEWV was trying to understand how it might work differently for this particular cohort. AGREED that: 1) the Quality Account-related update on Tees, Esk and Wear Valleys NHS Foundation Trust performance in 2023-2024, and the process for setting the 2024-2025 quality priorities, be noted. 2) a statement of assurance be prepared and submitted to the Trust, with final approval delegated to the Chair and Vice-Chair. 3) a letter be sent to the North East and North Cumbria Integrated Care Board (NENC ICB) supporting Hartlepool Borough Council's health scrutiny function in requesting clarity around how mental health Trusts ascertain patients sense of 'feeling safe' and the potential establishment of a baseline measure.
6	**North East Ambulance Service NHS Foundation Trust - Quality Account 2023-2024** A representative of North East Ambulance Service NHS Foundation Trust (NEAS) was in attendance to provide a presentation to the Committee in relation to the organisation's Quality Account, a document which NHS Trusts had a duty to produce each year. The NEAS Assistant Director – Communications and Engagement (who relayed apologies from the NEAS Deputy Director of Quality and Safety (Deputy Lead Nurse)) covered the following elements:

	➢ Overview of quality report requirements ➢ 2023/24 performance (1 April – 31 December 2023) o Patient safety o Patient experience and feedback o 999 incident volumes o Category 1 response performance (including benchmarking) o Category 2 response performance (including benchmarking) o Category 3 & 4 response performance (including benchmarking) o Hospital handover performance ➢ Update 2023/24 quality priorities Following a brief overview of the process requirements (consultation / publication) relating to the annual Quality Account (including that there was no obligation to obtain external auditor assurance this year), details were outlined on NEAS performance during the first three-quarters of 2023-2024 (April to December 2023). Regarding patient safety, the number of recorded serious incidents (140) was significantly higher than for the whole of 2022-2023 (61), though the criteria for what constituted a 'serious incident' had changed to a case where the required response time had been exceeded by more than one hour (it was noted that the recording of serious incidents was not consistent across the country, so benchmarking against other Trusts was not possible). For the 'proportion of safety incidents per 1,000 calls' measure, whilst the April to December 2023 figure (2.2%) was also up on the 2022-2023 data (1.8%), the final quarter for this year (January to March 2024) would likely reduce the overall rate for 2023-2024. In terms of patient experience and feedback, it was pointed out that the top three themes for complaints (staff attitude, timeliness of response, and quality of care) also appeared as themes for appreciations / compliments that NEAS received. Complaint numbers had been reducing since 2019-2020, and the number of appreciations for April to December 2023 (922) had already exceeded the number for the whole of 2022-2023 (812) and had surpassed the previous record (914) set in 2019-2020. 999 incident volumes between February 2023 and January 2024 (inclusive) had followed a similar trend for both the Tees Valley and Trust-wide footprint, with a broadly consistent number from March to November 2023, and a predictable increase in December 2023 and January 2024. For the most serious 'category 1' incidents (cardiac / respiratory arrest), Tees Valley performance compared favourably with the data for the entire NEAS patch, with mean response times consistently below the Trust-wide average for all months from February 2023 to January 2024. Whilst June 2023 and December 2023 saw NEAS go slightly above the average mean target response time (seven minutes) for category 1 cases, it was the only ambulance Trust in the country to be below this target in January 2024, something it was very proud of, and which reflected the significant amount of work which had been done around this measure.

	'Category 2' incidents (including strokes and heart attacks) comprised a large number of the overall contacts made to NEAS (around 70% of all calls) and, like all other ambulance Trusts across the country, mean response times were significantly above the target (18 minutes) for every month from February 2023 to January 2024 despite improvements compared to the previous year. Tees Valley mean response times were consistently worse than for the whole NEAS footprint (aside from January 2024) during the same period. Guidance around this measure was issued last year, with proposals to amend the target time from 18 minutes to 30 minutes. NEAS work around the provision of vehicle hours was outlined, with more crews put on the road than what the Trust had modelled (involving more vehicles / staff being taken on, including the recruitment of short-term assistance to aid response). A graphic demonstrated the actual number of vehicle hours compared to the Trust's operational plan (initiated in April 2023), with the impact on mean response times for category 2 cases against the revised 30-minute target shown. Whilst this presented a more positive picture, NEAS acknowledged that there was a clinical reason why the target was 18 minutes, something the Trust should not lose sight of. The average number of face-to-face incidents involving NEAS was charted, with these far exceeding planned numbers for every month from April 2023 onwards (including an all-time high in January 2024) – this raised the question of how the Trust managed such levels of demand without increased resources. It was noted that NEAS also operated patient transport crews which could be deployed to lower-level incidents where possible to free up paramedic crews. February 2023 to January 2024 performance for 'category 3' and 'category 4' (both urgent and non-urgent) cases was documented. Broadly speaking, Tees Valley response times (90th centile) were well above the targets for both (less so for the whole NEAS area, though still above target), results which were partially due to inefficiencies within the wider health system (i.e. delayed handovers at hospitals) and challenges in deploying staff with the right skills. To address the latter, NEAS was trying to develop / use Advanced Paramedic Practitioners (giving them more skills than standard ambulance crews) which aimed to benefit both patients (providing quicker care) and the whole 'system' (avoiding the need to take some individuals to hospital). Hospital handover data was included which illustrated the specific pressures at the James Cook University Hospital, Middlesbrough (a site which took in more patients due to having more speciality services). A rapid process improvement workshop was conducted to improve patient flow, and the Hospital Ambulance Liaison Officer (HALO) role had been re-introduced – such measures were working well and had been expanded across other areas of the NEAS footprint. Elsewhere, data showed rising handover delays towards the end of 2023 / start of 2024 at both the North Tees and Darlington hospitals (the latter seeing a marked increase in delays over two hours).

	The presentation concluded with commentary around what had been achieved, and what was still to do, in relation to the Trust's 2023-2024 quality priorities: • <u>To continue working with system partners to reduce handover delays (*Patient Safety*)</u>: Thematic analysis of handover delays undertaken, with particular focus on cases of moderate harm or below (had previously focused on more serious cases). Work with partners to improve data-sharing and standardise reporting (improving whole 'system' effectiveness) also completed. To begin addressing the need to understand the impact of handover delays on patients, an ambulance dataset had been introduced to start establishing outcomes for patients after handing them over (unaware of what happens to them currently) and ascertain the impact of hospital / ambulance interventions. This priority would not be carried forward to 2024-2025 but would instead become business-as-usual. • <u>Respond to patient safety incidents in a way that leads to service improvements and safer care for all our patients (*Patient Safety*)</u>: Several achievements noted, including a quality and safety profile review to inform local safety priorities, further development of governance procedures, transition to and training on PSIRF (Patient Safety Incident Response Framework), and the introduction of three patient safety partners. With regards work still to do, the Trust was on track to complete all serious incidents and actions by the end of March 2024. This priority would not be carried forward to 2024-2025 but assurance was given that NEAS would continue to focus on patient safety matters. • <u>Implementation of clinical supervision (*Clinical Effectiveness*)</u>: Policies and procedures had been developed, with an audit roadmap for Clinical Team Leaders (CTLs) introduced to understand individual clinical performance. Protected time for discussions was provided (particularly relevant for those crews / staff who were often working in isolation), with clinical staff also given five hours to support any development needs identified through supervision. Looking ahead, an electronic audit tool and dashboards were to be developed, as well as a bespoke university module to help ensure all CTLs have the appropriate skills, knowledge and experience (to be completed in 2024). This priority would not be carried forward to 2024-2025 but clinical effectiveness considerations would continue around 'Martha's Rule' (prompt access to a second opinion of an individual's condition). • <u>To increase service-user and colleagues' involvement in our patient safety and patient satisfaction activities (*Patient Experience*)</u>: NEAS Board, Trust partner, and stakeholder involvement in developments around this priority were highlighted, including the introduction of patient safety partners and the establishment of multi-disciplinary working groups for PSIRF implementation

and patient safety improvement activities. A patient feedback group still needed to be created, along with a patient and carer feedback survey (post-investigations), with wider involvement from patients and colleagues to be sought in relation to recruitment activities.

This priority would not be carried forward to 2024-2025 – NEAS would instead be focusing on the triangulation of data and making sense of the information it collected.

The Committee opened its reply to the presentation by probing those instances where patients were having to wait a significant time (beyond the target) for a response. NEAS stated that much of this had been as a result of staff capacity (the Trust had filled the roles for which it was funded for), though some could also be attributed to demand pressures and handover delays at hospitals. In terms of the latter, 30 minutes was the expected time for handover (15 minutes to pass the patient into the care of the hospital, and 15 minutes to re-stock) – the average for NEAS was 23 minutes, though this can increase during certain points of the year. It was noted that once handover delays begin, they can be very difficult to rein in.

Reflecting upon public awareness of the challenges in relation to ambulance response times / handover delays, Members asked if there was any evidence of people preferring not to make contact with NEAS and instead making their own way to hospital for treatment. The Committee was informed that the North East had benefitted from relatively stable relationships between health bodies which helped tackle pressure points more effectively than in other parts of the country.

Attention was drawn to the NHS 111 phoneline service, with the Committee querying if advice was consistent between that and the 999 number around who to contact in an emergency / non-emergency. NEAS advised that call-handlers across the region were dual-trained and that the same operators would answer whether 111 or 999 was used – the amount and order of questions may, however, be different depending on which number was dialled.

The Committee expressed concern that the positive developments around hospital handovers may slip if this was no longer an explicit priority for 2024-2025. NEAS gave assurance that the focus on ensuring timely handovers would not be lost (particularly since the issue had received national media interest) and that this was linked to the Trust's overriding commitment to patient safety. Members were also informed that the Secretary of State now received weekly briefings around this topic.

A question was raised about whether the Fire Brigade still acted as responders to 'category 3' incidents. NEAS stated that the Fire Brigade did not act as paramedics but did have a role as community first responders – as such, they will be dispatched to certain cases if available. The Committee also noted local schemes where different personnel were responding to certain incidents / environments (e.g. falls within care homes) – NEAS requested further details around these reported schemes if clarity was required.

	With reference to the use of additional staff, the Committee asked if NEAS had been supported with extra finance for recruitment. The Trust confirmed that commissioners had recognised the need for further resourcing and had provided significant additional funding to meet demand for services. The Committee concluded the session by emphasising that caution would be needed that the move to increasing the category 2 target response time to 30 minutes (instead of the previous 18-minute aim) did not negatively impact patient outcomes – Members were advised that this would be fed back to the relevant NEAS personnel to see if both targets could be monitored in the future (which may also aid national benchmarking), and that the Trust was trying to be smarter about how it categorised calls (this used to be done by clinicians but, following a pilot, was now classified at the point of the call being made by the call-handler (with clinical input if required)). Improved categorisation of incidents should help patients to receive better response times depending on their need. AGREED that… 1) the Quality Account-related update on North East Ambulance Service NHS Foundation Trust Quality Account performance in 2023-2024 be noted. 2) a statement of assurance be prepared and submitted to the Trust, with final approval delegated to the Chair and Vice-Chair.
7	**Work Programme 2023-2024** Consideration was given to the Committee's work programme for 2023-2024. Since this was the final meeting scheduled for the current municipal year, the Chair thanked Members for their contribution to the items which were considered during 2023-2024. As per the established rotational arrangements, support of the Committee would pass onto Hartlepool Borough Council for the 2024-2025 municipal year. AGREED that the Committee's work programme for 2023-2024 be noted.