Public Document Pack

James Ellis
Head of Legal and Democratic Services

MEETING	**:**	OVERVIEW AND SCRUTINY COMMITTEE
VENUE	**:**	COUNCIL CHAMBER, WALLFIELDS, HERTFORD
DATE	**:**	TUESDAY 21 MARCH 2023
TIME	**:**	7.00 PM

PLEASE NOTE TIME AND VENUE

This meeting will be live streamed on the Council's You Tube page: https://www.youtube.com/user/EastHertsDistrict

MEMBERS OF THE COMMITTEE

Councillor John Wyllie (Chairman)
Councillors M Brady, A Curtis, I Devonshire, H Drake, J Frecknall, M Goldspink (Vice-Chairman), D Hollebon, I Kemp, S Rutland-Barsby, D Snowdon, N Symonds and C Wilson

SUBSTITUTES

Conservative Group:	Councillors D Andrews and A Ward-Booth
Liberal Democrat Group:	Councillor S Bell
Labour:	Councillor C Redfern
Green:	Councillor B Crystall

(Note: Substitution arrangements must be notified by the absent Member to Democratic Services 24 hours before the meeting)

CONTACT OFFICER: PETER MANNINGS
01279 502174
PETER.MANNINGS@EASTHERTS.GOV.UK

Disclosable Pecuniary Interests

A Member, present at a meeting of the Authority, or any committee, sub-committee, joint committee or joint sub-committee of the Authority, with a Disclosable Pecuniary Interest (DPI) in any matter to be considered or being considered at a meeting:

- must not participate in any discussion of the matter at the meeting;
- must not participate in any vote taken on the matter at the meeting;
- must disclose the interest to the meeting, whether registered or not, subject to the provisions of section 32 of the Localism Act 2011;
- if the interest is not registered and is not the subject of a pending notification, must notify the Monitoring Officer of the interest within 28 days;
- must leave the room while any discussion or voting takes place.

Public Attendance

East Herts Council welcomes public attendance at its meetings and meetings will continue to be live streamed and webcasted. For further information, please email democraticservices@eastherts.gov.uk or call the Council on 01279 655261 and ask to speak to Democratic Services.

The Council operates a paperless policy in respect of agendas at committee meetings and the Council will no longer be providing spare copies of Agendas for the Public at Committee Meetings. The mod.gov app is available to download for free from app stores for electronic devices. You can use the mod.gov app to access, annotate and keep all committee paperwork on your mobile device.
Visit **https://www.eastherts.gov.uk/article/35542/Political-Structure** for details.

Audio/Visual Recording of meetings

Everyone is welcome to record meetings of the Council and its Committees using whatever, non-disruptive, methods you think are suitable, which may include social media of any kind, such as tweeting, blogging or Facebook. However, oral reporting or commentary is prohibited. If you have any questions about this please contact Democratic Services (members of the press should contact the Press Office). Please note that the Chairman of the meeting has the discretion to halt any recording for a number of reasons, including disruption caused by the filming or the nature of the business being conducted. Anyone filming a meeting should focus only on those actively participating and be sensitive to the rights of minors, vulnerable adults and those members of the public who have not consented to being filmed.

AGENDA

1. Apologies

   To receive apologies for absence.

2. Minutes - 8 November 2022 (Pages 6 - 16)

   To approve as a correct record the Minutes of the meeting held on 8 November 2022.

3. Chairman's Announcements

4. Declarations of Interest

   To receive any Members' Declarations of Interest.

5. Information Governance and Data Protection Policies (Pages 17 - 50)

6. East Herts Community Health and Wellbeing Plan 2023-2028

   Report 'to follow'

7. Air Quality Management Plan (Pages 51 - 74)

8. Regulation of Investigatory Powers Act (RIPA) Policy Review (Pages 75 - 155)

9. Overview and Scrutiny Committee - Draft Work Programme - 21 March 2023 (Pages 156 - 165)

10. Urgent Items

To consider such other business as, in the opinion of the Chairman of the meeting, is of sufficient urgency to warrant consideration and is not likely to involve the disclosure of exempt information.

MINUTES OF A MEETING OF THE OVERVIEW AND SCRUTINY COMMITTEE HELD IN THE COUNCIL CHAMBER, WALLFIELDS, HERTFORD ON TUESDAY 8 NOVEMBER 2022, AT 7.00 PM

PRESENT: Councillor J Wyllie (Chairman)
Councillors M Brady, A Curtis, I Devonshire, H Drake, J Frecknall, M Goldspink, D Hollebon, I Kemp, S Rutland-Barsby, D Snowdon, N Symonds and C Wilson

ALSO PRESENT:

Councillors G Cutting, J Goodeve and P Ruffles

OFFICERS IN ATTENDANCE:

Lorraine Blackburn	-	Scrutiny Officer
Lindsey Creed	-	Communications and Digital Media Manager
James Ellis	-	Head of Legal and Democratic Services and Monitoring Officer
Peter Mannings	-	Democratic Services Officer
Katie Mogan	-	Democratic Services Manager
Karen Page	-	The Service Manager (Development

		Management and Enforcement)
Sara Saunders	-	Head of Planning and Building Control
Tyron Suddes	-	Information Governance and Data Protection Manager
Ben Wood	-	Head of Communications, Strategy and Policy

198 APOLOGIES

There were no apologies.

199 MINUTES - 20 SEPTEMBER 2022

Councillor Goldspink proposed and Councillor Symonds seconded, a motion that the Minutes of the meeting held on 20 September 2022 be confirmed as a correct record and signed by the Chairman.

After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that the Minutes of the meeting held on 20 September 2022, be confirmed as a correct record and signed by the Chairman.

200 CHAIRMAN'S ANNOUNCEMENTS

There were no chairman’s announcements.

201 DECLARATIONS OF INTEREST

There were no declarations of interest.

202 DATA PROTECTION POLICY

The Executive Member for Corporate Services submitted a report that presented the newly drafted East Herts District Council Data Protection Policy. He invited Members to ask any questions they might have prior to the policy being submitted to the Executive for adoption.

The Overview and Scrutiny Committee Members asked some pre submitted and supplementary questions. The Executive Member for Corporate Services and the Information Governance and Data Protection Manager responded to these questions.

Councillor Devonshire proposed and Councillor Snowdon seconded, a motion that the Overview and Scrutiny Committee have considered the Data Protection Policy and recommend to the Executive that the policy be adopted.

After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that the Overview and Scrutiny Committee recommend to the Executive that the Data and Protection Policy be adopted.

203 SURVEILLANCE TECHNOLOGIES POLICY

The Executive Member for Corporate Services submitted a report that presented the newly drafted East Herts District Council Surveillance Technologies Policy. He invited questions from the Overview and Scrutiny Committee.

Councillor Goldspink expressed her thanks to Officers for their hard work on this report and on the previous report in respect of Data Protection. Councillor Symonds asked if Officers had any say or input into where police CCTV cameras were located.

The Executive Member for Corporate Services said that the council subscribed to the CCTV camera partnership. The Information Governance and Data Protection Manager advised that the council worked collaboratively with the police. He said that it was up to the police as the separate data controller and organisation to decide where CCTV surveillance cameras were located.

Councillor Rutland-Barsby proposed and Councillor Hollebon seconded, a motion that the Surveillance Technology Policy be adopted.

After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that the Overview and Scrutiny Committee recommend to the Executive that the Surveillance Technology Policy be adopted.

204 DEVELOPMENT MANAGEMENT UPDATE

The Executive Member for Planning and Growth submitted a report that set out the current position with planning applications. She said that the report explained the current challenges and actions being taken to improve the service and the steps being taken to address the backlog of planning applications and improve communications.

The Executive Member for Planning and Growth set out the numbers of applications being dealt with each year and said that significant and specialist resources were being allocated to the planning work associated with the allocated sites since the publication of the District Plan.

Members were advised that the volume of applications had increased significantly in the last two years in line with an identified national trend across the country. The Executive Member for Planning and Growth referred to a national shortage of planners and a high turnover of staff. She also referred to significant delays in responses from statutory consultees due to resource and recruitment challenges, which had also delayed planning decision making.

The Executive Member for Planning and Growth said that steps were being taken to address the backlog and speed up decision making in general. She said that

further interventions to speed up this process were summarised in the report.

The Overview and Scrutiny Committee Members asked some pre submitted and supplementary questions. The Executive Member for Planning and Growth and the Head of Planning and Building Control responded to these questions.

Councillor Snowdon asked if there were any organisations that could assist the council with other specific pieces or work relating to planning policy or the final details of section 106 agreements. The Head of Planning of Building Control said that there were a range of planning professionals that covered a whole range of planning services and functions. She said that the focus was development management and the resource within the planning policy team was stable. She emphasised the importance of planning officers being able to successfully negotiate the Section 106 agreements and the heads of terms on planning applications.

Councillor Curtis asked if the council had implemented any of the measures detailed at paragraph 3.4 of the report. The Head of Planning and Building Control said that a template had been devised and was being used by planning officers. Councillor Curtis said that the suggested changes and interventions should be implemented right away.

Members asked questions in respect of career graded posts and whether the salaries being paid were sufficiently competitive. The Head of Planning and

Building Control and the Executive Member for Planning and Growth confirmed that research had been carried out on the issue of salaries and also what the council could offer to Officers to develop their careers at East Herts and within Hertfordshire.

Councillor Wyllie asked if there were any improvements that Officers could request of Hertfordshire Highways to improve the East Herts planning process. The Service Manager (Development Management) said that there were regular meetings with Hertfordshire Highways. She said that early advice and intervention from Highways assisted officers in determining planning applications and the council did encourage applicants to engage with the pre application service offered by the Highway Authority.

Councillor Curtis proposed and Councillor Goldspink seconded, a motion that Overview and Scrutiny Committee have considered the content of the report and have provided observations to the Executive Member for Planning and Growth.

After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that Overview and Scrutiny Committee have considered the content of the report and have provided observations to the Executive Member for Planning and Growth.

205 DIGITAL COMMUNICATIONS UPDATE

The Executive Member for Corporate Services submitted a report inviting Overview and Scrutiny Committee to review progress against various elements of the East Herts Corporate Plan and the four "SEED" priorities.

The Overview and Scrutiny Committee Members asked some pre submitted and supplementary questions. The Executive Member for Corporate Services and the Head of Communications, Strategy and Policy responded to these questions.

Councillor Snowdon asked if email sign up could be used to encourage a wider circulation of the Network newsletter. He asked if the existing account set ups for business rates and council tax could include a sign-up option for Network. The Executive Member for Corporate Services said that good progress was being made with signing people up to the weekly newsletter. He undertook to mention this suggestion to officers.

Councillor Drake referred to paragraph 2.11 of the report and the increasing popularity of the call back option. She asked what could be done to further promote this facility and asked if there could be an option whereby people could leave a name, number and brief message for the council. The Head of Communications, Strategy and Policy said that the call back option was working well. He said that some extra comms work could be done to raise awareness and the new telephony system would allow messages to be left for the council.

Councillor Symonds said that not all people were able use digital services. She said that she was pleased to read that the council would support individuals who were not comfortable with or were unable to use digital services. She also commented on the problem of getting paperwork between Wallfields and Charringtons House via scanner or mobile phones.

The Executive Member for Corporate Services said that he would speak to officers in a review meeting next week and he would seek to get some answers to this ongoing issue. Councillor Goldspink expressed her concern over the target of answering 75 percent of calls within 10 minutes, which was a long time to wait. The Executive Member referred to plans for a new telephony system from 2023 and he mentioned that a new starter was about to start work with customer services.

The Head of Communications, Strategy and Policy and the Communications and Digital Media Manager provided some figures in respect of call volumes, Facebook followers and website hits following comments and a question from Councillor Kemp.

Councillor Snowdon proposed and Councillor Kemp seconded, a motion that the comments and suggestions be referred to the Executive.

After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that Overview and Scrutiny Committee refer the comments and suggestions to the Executive.

206 OVERVIEW AND SCRUTINY DRAFT WORK PROGRAMME

The Scrutiny Officer presented the draft work programme which was attached to the report as an appendix. She reminded Members of the scrutiny proposal form and invited the Committee to let her know of any training items in advance of the induction training planned for May 2023 for the cohort of Members.

The Scrutiny Officer referred to suggestions that Members had made in respect of the work programme going forward. Councillor Wilson spoke about Air Quality Management Areas (AQMAs) and the potential for improvements in the use of section 106 monies.

Councillor Wyllie commented on whether Hertfordshire County Councillors could attend the Overview and Scrutiny Committee. Members commented on concerns regarding parking standards in terms of whether parking was adequate on new developments. Councillor Wyllie emphasised that come May 2023 it would be the new Councillors on the Committee to shape the work programme.

It was proposed by Councillor Hollebon and seconded by Councillor Devonshire that the Committee Work Programme be approved. After being put to the meeting and a vote taken, the motion was declared CARRIED.

RESOLVED – that (A) the main agenda items for the next meeting be agreed; and

(B) the proposed Overview and Scrutiny Committee Work Programme be approved.

207 URGENT ITEMS

There was no urgent business.

The meeting closed at 8.20 pm

Chairman .....

Date .....

East Herts Council Report

Overview and Scrutiny Committee

Date of meeting: **Tuesday 21 March 2023**

Report by: **Councillor George Cutting – Executive Member for Corporate Services**

Report title: **Information Governance and Data Protection Policies Annual Review**

Ward(s) affected: **(All Wards);**

Summary – This report presents updates on the Access to Information Policy; the Data Breach Policy; and the Data Retention Policy as part of the annual policy review.

RECOMMENDATIONS FOR OVERVIEW AND SCRUTINY COMMITTEE

(A) The Committee considers the content of the report and amendments made to the policies and provides any observations to the Information Governance and Data Protection Manager.

1.0 Proposal(s)

1.1. This report provides an update on the Access to Information, Data Breach and Data Retention Policies as part of the annual policy review.

2.0 Background

2.1 Under paragraph 8.1.8 (n) of the Constitution, the Audit and Governance Committee has, as part of its terms of reference, a role to play in considering reports relating to the authority's Data Protection policies and procedures.

2.2 The Council is required to have appropriate information governance and data protection policies in place to demonstrate its accountability as required by the UK GDPR. These policies were last approved by Executive in 2021.

2.3 All policies required minor changes and these have been set out in paragraphs 2.3 to 2.5 below, apart from these amendments, the policies remain fit for purpose in all other regards.

General update

2.4 The Access to Information Policy has had minor amendments made to reflect new council policies and to clarify that exemptions will be considered rather than directly applied. Information has been summarised to make the policy more succinct.

2.5 The Data Breach Policy has had minor amendments made to reflect new council policies and learning from data breaches.

2.6 The Data Retention Policy has had some minor amendments made to reflect new council policies and has been updated to reflect storage locations of data, particularly in backup, following the council's migration to Microsoft 365.

3.0 Reason(s)

3.1 It is important that these policies are kept up to date to ensure that the council complies with developing information governance and data protection legislation and can demonstrate its accountability.

4.0 Options

4.1 To not annually review these policies, this is NOT RECOMMENDED as to do so would inevitably lead to the policies eventually becoming out of date and place the council in a position where it was potentially not meeting its legal obligations.

5.0 Risks

5.1 It is important that the council continues to operate in accordance with information governance and data protection legislation to ensure that it is able to effectively manage financial and reputation risks associated with non-compliance with this legislation.

6.0 Implications/Consultations

6.1 Not regularly reporting on the council's information governance and data protection compliance would risk it slipping out of the consciousness of Members.

Community Safety
No

Data Protection
Yes – keeping relevant policies updated ensures that the council remains compliant with data protection legislation.

Equalities
No

Environmental Sustainability
No

Financial
Not having up to date and legally compliant policies would place the council in a position of potentially falling foul of data protection legislation and facing fines of up to £8,700,000.

Health and Safety
No

Human Resources
No

Human Rights
No

Legal
Yes - The council is under an obligation to ensure it complies with information governance and data protection law, and keeping these policies updated strengthens the council's compliance with the relevant legislation.

Specific Wards
No

7.0 Background papers, appendices and other relevant material

7.1 **Appendix A** – Access to Information Policy with tracked changes

7.2 **Appendix B** – Data Breach Policy with tracked changes

7.3 **Appendix C** – Data Retention Policy with tracked changes

Contact Member
Councillor George Cutting, Executive Member for Corporate Services
george.cutting@eastherts.gov.uk

Contact Officer
James Ellis, Head of Legal and Democratic Services, Tel: 01279 502170. james.ellis@eastherts.gov.uk

Report Author
Tyron Suddes, Information Governance and Data Protection Manager, Tel: 01279 502148. tyron.suddes@eastherts.gov.uk

East Herts District Council

Access to Information Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Access to Information Policy
Author – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Date	October 2022
Approvals	Executive
Version	1.0
Next Review Date	October 2023

East Herts Council

Access to Information Policy

Contents

1. Policy Statement

East Herts Council ('the council') is committed to promoting and actively developing, a culture of openness, transparency and accountability embodied in the Access to Information legislation. This refers to the general right of access that the public have to the information held by the council. This right of access comes from the Access to Information legislation, namely:

- The Data Protection Act 2018 (DPA)
- The Environmental Information Regulations 2004 (EIR)
- The Freedom of Information Act 2000 (FOIA)
- The Re-use of Public Sector Information Regulations 2015 (RPSI).

This policy establishes a framework, which underlines this commitment and underpins the council's detailed guidance and procedures in the areas of Access to Information.

2. Purpose

This policy and the procedures which implement it will ensure that the council conforms to the Access to Information legislation and associated codes of practice, the key requirements of which are that:

- The lawful and correct treatment of personal information recognising the need to maintain confidence between the council and those with whom it deals.
- Information which is routinely published by the council will be made available in accordance with its publication scheme, and the Local Government Transparency Code 2014.
- Information which is not covered by the publication scheme is made available to applicants on request, within the statutory time limit, unless a valid exemption or exception applies.
- Exemptions or exceptions and/or charges under the FOIA, DPA and EIR are applied consistently and appropriately, and in accordance with the legislation.
- A fair and efficient internal appeal system is administered.

3. Responsibilities

3.1. The council has a corporate responsibility to ensure that it conforms to and implements the Access to Information legislation. The council is

accountable to the Information Commissioner for its compliance with this legislation.

3.2. The Information Governance and Data Protection Manager has a responsibility to ensure this policy is implemented, monitored and updated accordingly.

3.3. The Information Governance and Data Protection Manager and Information Officer are responsible for the effective day-to-day management of compliance with the legislation, including the:

- development of policies, procedures, guidance and standards of good practice and their dissemination to staff;
- maintenance and periodic review of the publication scheme;
- management of the information request processes within statutory timescales;
- disclosure of requested information and the consideration of exemptions or exceptions that prevent disclosure;
- provision of advice and assistance on access to information issues;
- promotion of good records management practices

3.4 An appointed member of staff within each service will act as a point of contact for access to information requests depending on the type of information requested. The point of contact will be responsible for the coordination, gathering and the forwarding of information to the Information Officer and/or Information Governance and Data Protection Manager for appraisal.

3.5 All staff must handle information and requests for information in a way that complies with this policy and the council's related procedures, guidance and standards of good practice. Staff should note that the deliberate concealment, amendment or destruction of information which has been the subject of a request, in order to prevent its disclosure, is a criminal offence under the Access to Information legislation for which individual staff as well as the council may be held liable.

4. Overview

4.1 Transparency

The council believes that transparency is a key condition and driver for the delivery of our services. As a publicly funded organisation, we have a duty to

be transparent in our business operations and outcomes in order to deliver value for money.

The council will publish information on its website, in accordance with the Local Government Transparency Code 2014. In addition, the council affirms its commitment to the routine publication of as much non-sensitive information about our policies, procedures and activities as possible.

4.2 The Freedom of Information Disclosure Log

The Freedom of Information Act 2000 requires public bodies to be proactive in the release of official information. As a result, the council has produced an online Freedom of Information Disclosure Log, which allows users to search a database, using keywords or categories, of previous Freedom of Information requests to ascertain whether their request may be similar.

4.3 Requests for information

Information which is not covered by the council's Freedom of Information Disclosure Log or which is not made routinely available can be requested by any individual, including corporate or public bodies under the FOIA and EIR. The legislation provides the public with the right to be informed whether the information is held by East Herts Council, and if so, to have the information communicated to them unless an exemption or exception applies. There is a maximum of 20 working days under the Access to Information legislation to provide the response or refusal notification. The deadline can be extended, but only in certain circumstances.

A data subject's personal information can be requested under the DPA and the Council has a maximum of 1 month in which to process a request unless an exemption applies. The deadline for response can be extended to a maximum of 2 further months for large or complex requests.

The council is committed to processing requests for information in accordance with the requirements of the applicable legislation. The council will ensure that requests are processed in accordance with the Code of Practice issued by the Secretary of State at the Ministry of Justice under section 45 of the Freedom of Information Act. Similarly, requests under the Environmental Information Regulations will be handled according to the Code of Practice issued by the Department for Environment, Food and Rural Affairs.

Procedures and systems for dealing with information requests have been developed to promote conformity to these codes and the legislation, and will be coupled with appropriate training for staff handling requests. Subject access requests will be processed under the DPA according to the Data Protection Principles.

4.4 Charges

Whilst the council does not normally charge for information requests, it still needs to be able to calculate how much a request would 'cost' to determine if the request is excessive and/or puts a strain on council resources. The FOIA imposes a statutory limit on the amount that can be spent on locating and extracting the information required to answer a request. This limit is currently set at £450.00, which equates to 2.5 days of staff time.

When estimating the cost of complying with a request for information, the council can take into account the staff time reasonably incurred, when involved in the following activities:

- determining whether the council holds the information;
- locating the information or a document which may contain the information;
- retrieving the information, or a document that may contain the information;
- extracting the information from a document containing it

The following actions will be taken once the estimated cost has been determined:

- If the request is estimated to amount to less than £450.00 of work (less than 2.5 days), the council will respond to the request at no cost.
- If the request is estimated to amount to in excess of £450.00 of work (more than 2.5 days); the council may consider the appropriate exemption or exception or the requestor may incur a fee in line with the council's access to Information fees.

Prior to charging for an information request or considering an exemption or exception, the council will provide the applicant with reasonable advice and assistance to refine or narrow down the request.

4.5 Exemptions or exceptions

Although the council upholds the principle that information should be accessible wherever possible; there are times when it has to withhold information to protect

its legitimate interests and those of other organisations and individuals. The council will only refuse to disclose information in response to a request if a valid exemption or exception applies under the FOIA, DPA or the EIR.

Where information is withheld, requestors will be informed of the relevant exemption or exception and why the council believes it applies, including if necessary, consideration of the public interest test. Applicants will be provided with details of the relevant review and complaint procedures.

The Information Officer and/or Information Governance and Data Protection Manager must be consulted in all cases where staff believe that the release of the requested information is felt to be inappropriate so that an appropriate exemption or exception can be considered.

The Information Officer or Information Governance and Data Protection Manager will appraise the information against the available exemption(s) or exception(s) in order to decide whether or not one is applicable.

4.6 Access to Information review procedures

The Council will provide an internal review process against initial responses to requests for information. The review will be conducted in accordance with section 45 of the FOIA or Regulation 11 of the EIR.

This procedure will be followed if an applicant expresses dissatisfaction, whether justified or not about the way their request was handled and about the information supplied or not supplied.

Following ICO good practice guidance, the council will conduct an internal review where requested by the applicant in relation to reliance on a data subject right.

Applicants can appeal to the Information Commissioner if they remain dissatisfied after going through an internal review procedure.

4.7 Third Parties

This policy covers all information held by the council or information held on its behalf, including information provided to us by third parties such as contractors,

tenderers, suppliers, other public or regulatory bodies. The council does not have to consult with third parties on every occasion, however, there may be occasions when the council feels it is necessary, for example due to the type of information requested, the relationship the council has with the third party or any previous notification that information may be confidential.

4.8 Re-Use of Information

Requests may be made to the council for the re-use of information under the Re-use of Public Sector Information Regulations 2015 (RPSI). These regulations apply to information that the council produces as part of its public task. Information held that is not part of the council's public task is not covered by RPSI.

RPSI should not be confused with other Access to Information legislation, i.e. the DPA, FOIA or EIR apart from the fact that RPSI does not apply to information that would be exempt from disclosure under this legislation.

Re-Use, in this context, means using public sector information for a purpose other than the initial public task it was produced for. Typically, this would mean the requestor taking the information produced and republishing it or using it to produce a new product or resource, often by combining it with other information, sometimes on a commercial basis. RPSI aims to permit and encourage the re-use of information and how it is made available as opposed to accessing information, which is dealt with under the information access legislation above.

4.8.1. Requests for re-use

A request for re-use must be made in writing, with the requestor's name and address for correspondence, and must specify the information they want to re-use and the purpose they intend to use it for.

When a request is received, the council will respond within 20 working days, unless there is a need to extend this time where the information is extensive or the request raises complex issues. The council will inform the requestor of any delay within the 20 day period. If the requested information has not previously been disclosed then the council will, additionally, deal with the request as an access request under the appropriate legislation in order to decide whether the information is exempt.

The council will ensure that the information for re-use is made available in the format and language in which it is held and, where required, will make the information available in an open and machine readable format where it is not held in such a way.

The council may impose conditions on re-use but the conditions must be as open and non-restrictive as possible.

4.8.2. Charges for re-use

The council may charge for the marginal costs of reproducing, providing and disseminating information where this is excessive or where the council is required to generate revenue to cover:

- A substantial part of the costs relating to the public task;
- Documents for which the council is required to generate revenue to cover a substantial part of the costs;

In most cases, the above costs will be negligible and no charge will be made. Additionally, if the information is published on the council's website, then it is unlikely that a charge will be made.

If a charge is made, then the council will use regulation 15 of RPSI to determine how the charge should be calculated.

4.8.3. Review procedures

The council will use its internal review process against any complaints received about how it handled a request for re-use. The complaint should be submitted to the council in writing and the council will review its original decision and respond to the complaint within a reasonable time.

5. Help and Assistance

Please contact either the Information Governance and Data Protection Manager or Information Officer if you need help or assistance.

Alternatively, you may find that the following resources available on the council's intranet may help:

- GDPR and Data Protection

East Herts District Council

Data Breach Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Data Breach Policy
Author – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Date	October 2022~~July 2021~~
Approvals	Executive
Version	1.1
Next Review Date	~~July 2021~~October 2023

Contents

1. Introduction

This Policy sets out the obligations of East Hertfordshire District Council ("the Council") regarding the handling and reporting of data breaches and personal data breaches in accordance with UK Data Protection Legislation. "Data Protection Legislation", in this Policy, means all legislation and regulations in force from time to time regulating the use of personal data including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, and any successor legislation.

The UK GDPR defines "Personal Data" as any information relating to an identified or identifiable natural person (a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The UK GDPR defines a "Personal Data Breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

The Council is under a duty to report certain types of Personal Data Breach directly to the Information Commissioner's Office ("ICO"). The Council is also required to inform individual Data Subjects in the case of breaches that present a high risk of adversely affecting their rights and freedoms.

All personal data collected, held, and processed by the council will be handled in accordance with the Council's ~~Policy for Handling Personal Data.~~Data Protection Policy.

The Council has in place procedures for the detection, investigation, and reporting of data breaches. This Policy applies to all data breaches (including personal data breaches) within the Council and is designed to assist in both the handling of such breaches and in determining whether or not they must be reported to the ICO and/or to Data Subjects.

The Council's Information Governance and Data Protection Manager and Information Officer are responsible for overseeing the handling of all data breaches. The Council's Leadership Team, line managers and Information Governance and Data Protection Manager are responsible for the implementation of this Policy and ensuring that this Policy is adhered to by all staff.

2. Scope of Policy

2.1 This Policy relates to all forms of data (including personal data and sensitive personal data (known as "special category" under the Data Protection Legislation)) collected, held, and processed by the Council.

2.2 This Policy applies to all staff and elected members of the Council, including but not limited to employees, agents, contractors, consultants, temporary staff, casual or agency staff, or other suppliers or data processors working for or on behalf of the Council.

2.3 This Policy applies to all data breaches, whether suspected or confirmed.

3. Data Breaches

3.1 For the purposes of this Policy, a data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of data.

3.2 Incidents to which this Policy applies may include, but not be limited to:

3.2.1 the loss or theft of a physical data record;

3.2.2 the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;

3.2.3 equipment failure;

3.2.4 unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);

3.2.5 unauthorised disclosure of data;

3.2.6 human error (e.g. sending data to the wrong recipient);

3.2.7 unforeseen circumstances such as fire or flood;

3.2.8 hacking, phishing, and other 'blagging" offences whereby information is obtained by deception.

4. Internal Reporting

4.1 If a data breach is discovered or suspected, members of staff should immediately notify their line manager and complete a Staff Data Breach Report Form (available on the Council's intranet) which will be sent to the Council's Information Officer and/or Information Governance and Data Protection Manager. If considered necessary due to the nature of the breach, it should be reported to IT Services via the ICT Help Desk (ext. 2249).

4.2 Members should complete a Staff Data Breach Report form and send the completed form to the Council's Information Officer and/or Information Governance and Data Protection Manager and if considered necessary, IT should be notified.

4.3 A completed Staff Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

4.3.1 the time and date the breach was discovered;

4.3.2 the type(s) of data involved;

4.3.3 where the breach involves personal data, the categories(s) of data subject to which the personal data relates (e.g. customers, employees etc.);

4.3.4 whether or not any sensitive personal data is involved;

4.3.5 how many Data Subjects are likely to be affected (if known);

4.3.6 details of what may have caused the breach;

4.3.7 details of any immediate actions taken to reduce the impact of the breach.

4.4 If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable to keep within the **72 hour limit** imposed by Data Protection Legislation. Staff should keep in mind that some time may be needed to minimise the effect of the potential data breach.

4.5 Unless and until instructed to by the Information Governance and Data Protection Manager or a Head of Service, no further action should be taken with respect to a data breach. In particular, individual members of staff should not take it upon themselves to notify affected Data Subjects, the ICO, or any other individuals or organisations.

5. Initial Management and Recording

5.1 Upon receipt of a Staff Data Breach Report Form (or upon being notified of a data breach in any other way), the Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or their line manager shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

5.2 Having established the above, the following steps shall then be taken by the parties mentioned in 5.1 above with respect to the data breach:

5.2.1 undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the likelihood and severity of the data breach. This is will be determined on a case by case basis and may include, but is not limited to, consideration of the number of Data Subjects and sensitivity of personal data involved;

5.2.2 With assistance from IT if required, contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;

5.2.3 determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

5.2.4 establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;

5.2.5 determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and

5.2.6 record the breach and the initial steps taken above in the Council's Data Breach Log.

5.2.7 Having completed the initial steps described above, the Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or line manager shall proceed with investigating and assessing the data breach as described in Part 6, below.

6. Investigation and Assessment

6.1 The Information Governance and Data Protection Manager and/or Information Officer and relevant member(s) of staff and/or line manager shall begin an investigation of a data breach as soon as is reasonably possible after receiving a Staff Data Breach Report Form (or being notified in any other way) and, in any event, within **24 hours** of the data breach being discovered and/or reported.

6.2 Investigations and assessments may take the following into account:

6.2.1 the type(s) of data involved (and, in particular, whether the data is personal data or sensitive/special category personal data);

6.2.2 the sensitivity of the data (both commercially and personally);

6.2.3 what the data breach involved;

6.2.4 what organisational and technical measures were in place to protect the data;

6.2.5 what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);

6.2.6 where personal data is involved, what that personal data could tell a third party about the Data Subjects to whom the data relates;

6.2.7 the category or categories of data subject to whom any personal data relates;

6.2.8 the number of Data Subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;

6.2.9 the potential effects on the Data Subjects involved;

6.2.10 the potential consequences for the Council;

6.2.11 the broader consequences of the data breach, both for Data Subjects and for the Council;

6.3 The results of the investigation and assessment described above must be recorded in a Data Breach Report and a summary noted in the Council's Data Breach Log.

6.4 Having completed the investigation and assessment described above, the

Information Governance and Data Protection Manager and/or Information Officer in liaison with the relevant member(s) of staff and/or line manager**,** shall determine the parties to be notified of the breach as described in Part 7~~6~~, below.

7. Internal Notification

7.1 If not already aware, the Head of Service of the affected service area shall be made aware of all data breaches regardless of the level of risk.

7.2 The Information Governance and Data Protection Manager and/or Information Officer in liaison with the relevant member of staff and/or line manager shall determine whether to notify one or more of the following parties of the breach:

7.2.1 Senior Information Risk Officer (SIRO);

7.2.2 Deputy Chief Executive and/or Chief Executive;

7.2.3 Head of Communications and Leader of the Council (if not already notified)

7.2.4 affected Data Subjects;

7.2.5 the ICO;

7.2.6 the police;

7.2.7 affected third parties;

7.2.8 IT (if not already notified).

7.3 When considering whether to notify the SIRO, Deputy Chief Executive, Chief Executive or affected third parties, the nature of the breach and the severity of the impact it may have on Data Subjects should be taken into account. All data breaches deemed medium to high risk should immediately be brought to the attention of these parties.

~~7.3~~7.4 The Council's Leadership Team and Audit and Governance Committee will be made aware of all data breaches regardless of risk level on a half yearly basis through a data breach summary report.

~~7.4~~7.5 If not already aware, the Head of Communications and Leader of the Council should be made aware of any high risk breaches so that they can be appropriately briefed if approached by the media for comment.

8. External Notification

8.1 When considering whether (and how) to notify individual Data Subjects in the event of a personal data breach, the following should be considered:

8.1.1 the likelihood that Data Subjects' rights and freedoms as set out in the Data Protection Legislation (and the Council's ~~Policy for Handling Personal Data~~Data Protection Policy) will be adversely affected;

8.1.2 whether there is a legal or contractual requirement to notify;

8.1.3 whether measures in place to protect the affected personal data (e.g. pseudonymisation or encryption) have been applied, thereby rendering the data unusable to any unauthorised parties;

8.1.4 whether measures have been taken following the data breach that will ensure that a high risk to the rights and freedoms of affected Data Subjects is no longer likely to occur;

8.1.5 the benefits to Data Subjects' of being notified (e.g. giving them the opportunity to mitigate the risks posed by the data breach);

8.1.6 whether notifying individuals will involve disproportionate effort (in which case a public communication or other widely available notice may suffice, provided that affected Data Subjects will still be informed effectively);

8.1.7 the best way of notifying Data Subjects, taking into account the urgency of the situation and the security of the possible methods;

8.1.8 any special considerations applicable to certain categories of data subject (e.g. children or vulnerable people);

8.1.9 the information that should be provided to affected Data Subjects;

8.1.10 how to make it easy for affected Data Subjects to contact the Council to find out more about the data breach;

8.1.11 further assistance that the Council should provide to the affected Data Subjects, where appropriate;

8.1.12 the risks of over-notifying – not all data breaches require notification and excessive notification may result in disproportionate work and numbers of enquiries from individuals and undue stress placed on those individuals;

8.2 When individual Data Subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

8.2.1 a user-friendly description of the data breach, including how and when it occurred, the personal data involved, and the likely consequences;

8.2.2 clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

8.2.3 a description of the measures taken (or proposed to be taken with estimated dates) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;

8.2.4 contact details for Information Governance and Data Protection Manager and relevant member(s) of staff from whom affected individuals can obtain further information about the data breach.

8.3 When considering whether (and how) to notify the ICO of a data breach, the following should be considered:

8.3.1 the likelihood of risk and potential harm to Data Subjects, their rights, and freedoms – harm can include (but is not limited to) financial harm, physical harm, loss of control over personal data, discrimination, identity theft or fraud, damage to reputation, and emotional distress;

8.3.2 the volume of personal data involved – the ICO should be notified if a large volume of data is involved and there is a real risk of Data Subjects suffering harm as a result, however it may also be appropriate to notify the ICO if a smaller amount of high-risk data is involved;

8.3.3 the sensitivity of the data involved – the more sensitive the personal data is, the less the volume of it is relevant and if the data breach presents a significant risk of Data Subjects suffering substantial detriment or distress, the ICO should be notified.

8.4 If the ICO is to be notified of a data breach, this must be done within **72 hours** of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The ICO must be provided with the following information:

8.4.1 the category or categories and the approximate number of data subject whose personal data is affected by the data breach;

8.4.2 the category or categories and the approximate number of personal data records involved;

8.4.3 the name and contact details of the Information Governance and Data Protection Manager from which the ICO can obtain further information about the data breach;

8.4.4 a description of the likely consequences of the data breach; and

8.4.5 a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

8.5 The police may have been contacted at an earlier point in the data breach procedure (see 54.2), however further investigation may reveal that the data breach resulted from a criminal act, in which case the police should be further informed.

8.6 Records must be kept of all data breaches, regardless of whether notification is required. The decision-making process surrounding notification should be documented and recorded in a Data Breach Report and a summary noted in the Data Breach Log.

9. Evaluation and Response

9.1 When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the Information Governance and Data Protection Manager and/or Information Officer and/or relevant member(s) of staff, their line manager and, if required, the relevant Head of Service shall conduct a complete review of the causes of the data breach, the

effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future. Additionally, where breaches have not been escalated, these will be reported via the half yearly meetings as mentioned in paragraph 7.46.3 above in order to determine if improvement is required. Any recommendations and/or actions made through a review, if applicable, will be shared with all council staff as soon as possible through regular data protection best practice updates on the intranet. .

9.2 Such reviews shall, in particular, consider the following with respect to data (and in particular, personal data) collected, held, and processed by the Council:

9.2.1 where and how data is held and stored;

9.2.2 the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;

9.2.3 the methods of data transmission for both physical and electronic data and whether or not such methods are secure;

9.2.4 the level of data sharing that takes place and whether or not that level is necessary;

9.2.5 whether any data protection impact assessments need to be conducted or updated;

9.2.6 staff awareness and training concerning data protection;

9.3 Where possible improvements and/or other changes are identified, the Information Governance and Data Protection Manager shall liaise with the relevant member(s) of staff, their line manager and, if required, the relevant Head of Service with respect to the implementation of such improvements and/or changes.

9.4 Any actions taken against an employee found to be responsible for a confirmed data breach shall be in line with the Council's Disciplinary Policy and should be treated as a general misconduct breach of the Council's Code of Conduct.

East Herts District Council

Data Retention Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Retention Policy
Author – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Owner – name and title	Tyron Suddes, Information Governance and Data Protection Manager
Date	October 2022~~July 2021~~
Approvals	Executive
Version	1.0
Next Review Date	~~July 2022~~October 2023

Contents

1. Introduction

This Policy sets out the obligations of East Hertfordshire District Council ("the Council") regarding retention of personal data collected, held, and processed by the Council in accordance with Data Protection Legislation. "Data Protection Legislation" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

Data Protection Legislation defines "personal data" as any information relating to an identified or identifiable natural person (a "Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data Protection Legislation also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under Data Protection Legislation, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by Data Protection Legislation to protect that data).

In addition, Data Protection Legislation includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

1.1. Where the personal data is no longer required for the purpose for which it was originally collected or processed;

1.2. When the data subject withdraws their consent;

1.3. When the data subject objects to the processing of their personal data and the Council has no overriding legitimate interest;

1.4. When the personal data is processed unlawfully (i.e. in breach of Data Protection Legislation or any other legislation);

1.5. When the personal data has to be erased to comply with a legal obligation;

or

1.6. Where the personal data is processed for the provision of information society services to a child.

This Policy governs the Council's ~~separate~~ Data Retention Schedule which sets out the type(s) of personal data held by the Council's services for specific purposes, the period(s) for which that personal data is to be retained and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with Data Protection Legislation, please refer to the Council's ~~Policy for Handling Personal Data~~Data Protection Policy.

2. Aims and Objectives

2.1. The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Council complies fully with its obligations and the rights of data subjects under the Data Protection Legislation.

2.2. In addition to safeguarding the rights of data subjects under the Data Protection Legislation, by ensuring that excessive amounts of data are not retained by the Council, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by all service areas within the Council and by third-party data processors processing personal data on the Council's behalf.

3.2 Personal data, as held by the above is stored in the following ways and in the following locations:

3.2.1 The Council's servers, located in Stevenage;

3.2.2 Third-party approved cloud hosting solutions ('The Cloud,)~~servers~~, operated by the Council's service providers;

3.2.3 Computers permanently located in the Council's premises at Wallfields, Pegs Lane, Hertford and Charringtons House, The Causeway, Bishops Stortford;

3.2.4 Laptop computers and other mobile devices provided by the Council to its employees;

3.2.5 Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Council's ICT user policies;

3.2.6 Physical records stored in the Council's premises;

3.2.7 and all off-site archives used by the Council

4. Data Subject Rights and Data Integrity

4.1. All personal data held by the Council is held in accordance with the requirements of Data Protection Legislation and data subjects' rights thereunder, as set out in the Council's ~~Policy for Handling Personal Data~~Data Protection Policy.

4.2. Data subjects are kept fully informed of their rights, of what personal data the Council holds about them, how that personal data is used, and how long the Council will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3. Data subjects are given control over their personal data held by the Council including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by the Council's Data Retention Schedule), the right to restrict the Council's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1. The Council aims to ensure that all of the following technical measures are in place to protect the security of personal data:

5.1.1 All emails ~~containing~~ used to share personal data must be encrypted;

5.1.2 All emails ~~containing~~ used to share personal data must be marked "confidential";

5.1.3 Personal data may only be transmitted over secure networks;

5.1.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

5.1.5 Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient

5.1.6 All personal data transferred physically should be transferred in a suitable container marked "confidential";

5.1.7 No personal data may be shared informally and if access is required to any personal data, such access should be requested from the relevant data administrator

5.1.8 All hardcopies of personal data, along with any electronic copies

stored on physical media should be stored securely;

5.1.9 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation;

5.1.10 Personal data must be handled with care at all times and should not be left unattended or on view;

5.1.11 Computers used to view personal data must always be locked before being left unattended;

5.1.12 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Council where the party in question has agreed to comply fully with the Council's ~~Policy for Handling Personal Data~~Data Protection Policy and the Data Protection Legislation;

5.1.13 All personal data stored electronically should be backed up regularly with backups stored onsite **AND/OR** offsite. All backups should be encrypted;

5.1.14 All electronic copies of personal data should be stored securely using passwords and encryption;

5.1.15 All passwords used to protect personal data should be changed regularly and must be secure;

5.1.16 Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method;

5.1.17 All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

5.1.18 No software may be installed on any Council-owned computer or device without approval; and

5.1.19 Where personal data held by the Council is used for marketing purposes, it shall be the responsibility of the relevant data administrator to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

5.2 The Council aims to ensure that the following organisational measures are in place to protect the security of personal data:

5.2.1 All employees and other parties working on behalf of the Council shall be made fully aware of both their individual responsibilities and the Council's responsibilities under the Data Protection Legislation

and under the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.2 Only employees and other parties working on behalf of the Council that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Council;

5.2.3 All employees and other parties working on behalf of the Council handling personal data will be appropriately trained to do so;

5.2.4 All employees and other parties working on behalf of the Council handling personal data should exercise care and caution when discussing any work relating to personal data;

5.2.5 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

5.2.6 All employees and other parties working on behalf of the Council handling personal data will be bound by contract to comply with the Data Protection Legislation and the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.7 All agents, contractors, or other parties working on behalf of the Council handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Council arising out of the Data Protection Legislation and the Council's ~~Policy for Handling Personal Data;~~Data Protection Policy;

5.2.8 Where any agent, contractor or other party working on behalf of the Council handling personal data fails in their obligations under the Data Protection Legislation and/or the Council's ~~Policy for Handling Personal Data,~~ Data Protection Policy, that party shall indemnify the Council against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

6.1. Upon the expiry of the data retention periods set out in the Council's Data Retention Schedule, or when a data subject exercises their right to have their personal data erased and this is upheld by the Ccouncil, personal data shall be anonymised deleted, destroyed, or otherwise disposed of as follows:

6.1.1. Personal data stored electronically (including any and all backups thereof) shall be deleted securely by the user. This will be followed by a 30 day soft deletion delay until the personal data is permanently deleted ;

6.1.2. Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely by the user. This will be followed by a 30 day soft deletion delay until the personal

data is permanently deleted;

6.1.3. Personal data stored in hardcopy form shall be disposed of in the Council's confidential waste bins;

6.1.4. Special category personal data stored in hardcopy form shall be disposed of in the Council's confidential waste bins;

6.1.5. If appropriate, both personal and special category shall be made truly anonymous so that it is no longer in a form which permits identification of data subjects.

7. Data Retention

7.1. As stated above, and as required by law, the Council shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in the Council's Data Retention Schedule.

7.3. When establishing and/or reviewing retention periods, the following shall be taken into account:

7.3.1. The objectives and requirements of the Council;

7.3.2. The type of personal data in question;

7.3.3. The purpose(s) for which the data in question is collected, held, and processed;

7.3.4. The Council's legal basis for collecting, holding, and processing that data;

7.3.5. The category or categories of data subject to whom the data relates;

7.3.6. The technical and organisational security measures in place;

7.3.7. The Local Government Association's data retention schedule guidance.

7.3.8. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.3.9. Notwithstanding defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Council to do so (whether in response to a request by a data subject or otherwise).

7.3.10. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving

purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the UK GDPR.

8. Roles and Responsibilities

8.1. The Council's Data Protection Officer is the Information Governance and Data Protection Manager and can be contacted by emailing data.protection@eastherts.gov.uk

8.2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with it, the Council's other Data Protection-related policies and with Data Protection Legislation.

8.3. The relevant data administrator(s) shall be directly responsible for ensuring compliance with data retention periods within their service areas

8.4. Any questions regarding this Policy, the retention of personal data, or any other aspect of Data Protection Legislation compliance should be referred to the Data Protection Officer.

East Herts Council Report

Overview and Scrutiny Committee

Date of meeting: 21 March 2023

Report by: Councillor Graham McAndrew, Executive Member for Environmental Sustainability

Report title: Air Quality in East Herts

Ward(s) affected: All

Summary

- This report aims to address questions raised by members of the Overview and Scrutiny Committee at their last meeting around the council's air quality management areas and air quality action plan.

RECOMMENDATIONS FOR OVERVIEW AND SCRUTINY COMMITTEE:

a) Members scrutinise the council's work in relation to air quality and more specifically the three air quality management areas so as to consider the extent to which the council is using available resources to have a positive impact on public health, with any comments passed to the Executive Member for Environmental Sustainability; and

b) Members scrutinise the council's work in relation to air quality so as to consider the extent to which the council is fulfilling its statutory obligations with regards to the three air quality management areas, with any comments passed to the Executive Member for Environmental Sustainability.

1.0 Background

1.1 At its last meeting, members of the Overview and Scrutiny Committee requested clarification on the work the council is undertaking to improve air quality in East Herts and revoke the air quality management areas (AQMA) in Bishop's Stortford, Hertford and Sawbridgeworth. Members specifically asked:

a) is the air quality action plan being followed and is it fit for purpose?
b) is our website advertising the issues sufficiently to our residents?
c) are we fulfilling our statutory duties?
d) have the new housing developments had a negative impact on the existing AQMAs?
e) have 'Section 106' monies coming from those developments been used as they should have been with regards to air quality?

1.2 This report will address these points and demonstrate the important air quality work being carried out across the council.

1.3 For the purposes of this report, unless stated otherwise, all references to information on our website refer to our dedicated air quality page which can be found here - https://www.eastherts.gov.uk/environmental-health/air-quality

2.0 Monitoring air quality in East Herts

2.1 At present, the council has 48 nitrogen oxides diffusion tubes across 34 sites in the district and one fixed continuous air quality monitor in Hertford.

2.2 Nitrogen oxides diffusion tubes, also known as 'NOx tubes', are a cost effective, long-term monitoring option used by local authorities across the UK.

2.3 The NOx tubes have been placed in areas where there are known problems with air quality and areas where there is expected to be large development over the coming years, such as Buntingford. The list of current diffusion tube locations can be found on our website within our air quality Annual Status Report (ASR).

2.4 While the ASR also contains data relating to the continuous air quality monitor in Hertford, access to 'live' data from this monitor, along with other data from across Hertfordshire and Bedfordshire can be found on our dedicated website https://www.airqualityengland.co.uk/site/latest?site_id=HB012

3.0 Air Quality Management Areas

3.1 An air quality management area (AQMA) is declared for an area where the local air quality is unlikely to meet the Government's national air quality objectives.

3.2 Once an AQMA has been declared, the council has to carry out further work to monitor the air quality in the area and identify what action can be taken to improve it. This work then leads to the publication of an Air Quality Action Plan.

3.3 The National Air Quality Strategy sets air quality objectives which are designed to protect the health of the public. If these levels are exceeded, health effects could be felt, particularly for those people with certain respiratory health conditions.

3.4 There are two air quality objectives for nitrogen dioxide; one to protect residents and others who will be breathing the air for a long time and one to protect visitors who are just passing

through the area.

a) The long-term objective (for residents) is 40ug/m^3 averaged over a year.

b) The short-term objective (for visitors) is 200ug/m^3 averaged over one hour.

3.5 As mentioned above, the council has three AQMAs in the district. One in Bishop's Stortford, one in Hertford and more recently one in Sawbridgeworth.

a) Bishop's Stortford was the council's first AQMA to be declared back in February 2007. It covers the area in and around Hockerill Junction.

b) Hertford was the council's second AQMA to be declared back in 2010. It covers the area along and around the A414 (Gascoyne Way) as it passes through Hertford.

c) Sawbridgeworth was the council's third AQMA to be declared back in 2015. It covers the area along and around the A1184 (London Road) as it passes through Sawbridgeworth.

3.6 Maps and further details outlining the exact areas covered are published on the Department for Environment Food and Rural Affairs (Defra) website, with links to them from our website.

4.0 Air Quality Action Plan

4.1 The council's most recent air quality action plan was published in 2017, with timetable actions running until 2020. This is available on our website and was reviewed regularly during the period leading up to the COVID Pandemic.

4.2 The action plan identified 39 individual actions which it was posited would positively impact the air quality in one or more of the AQMAs or more generally improve air quality across the district.

4.3 Of the 39 actions, 23 have been confirmed as having been achieved. The remaining actions are under way with our external partners.

4.4 The emergence of the COVID Pandemic in 2020 resulted in Environmental Health as a whole, and most definitely in East Herts, being re-tasked to work on local, regional and national COVID-related work given the unprecedented nature of this public health emergency. Unfortunately, one impact of this was that the work on reviewing and refreshing the Air Quality Action Plan had to be delayed and so while this work has now recommenced, the council is currently without a more recently published action plan than the one running until 2020.

4.5 Since 2020, work on tackling air quality has in fact continued at pace. More details are outlined in Section 0 below.

4.6 As part of the business recovery following the pandemic designed in some ways to 'make up for lost time' on key areas of the Environmental Health workload, the council commissioned a specialist company, Bureau Veritas, in March 2022 to assist with the creation of a new air quality action plan. Their remit was to:

a) Undertake a source apportionment exercise to help identify the sources of pollution within the AQMAs and so aid the design of appropriate mitigation actions. Then use this data to inform suitable air quality action measures.

b) Bring external partners together to create a shared action plan which will lead to the revocation of the three air

quality action plans.

4.7 Bureau Veritas have now completed the source apportionment and have begun working with the officers from across the council and our key partners, notably Hertfordshire County Council, to draw up a new action plan. This work is anticipated to be completed during the latter half of 2023/24.

5.0 New Air Quality Action Plan timetable

5.1 As mentioned in Section 0 above, work is now underway on preparing the next Air Quality Action Plan for East Herts. Assuming there are no unexpected delays, it is anticipated that the following timeline can be achieved:

- **By the end of April 2023** – Officers from East Herts Council, Hertfordshire County Council, Bureau Veritas and other key partners will produce a draft action plan.

- **By the end of May 2023** – The draft action plan will be circulated to the public and key partners as part of a consultation exercise.

- **By the end of September 2023** – Overview and Scrutiny Committee will have had an opportunity to consider the final draft action plan and make recommendations to the Executive Member for Environmental Sustainability.

- **By the end of January 2024** – Air Quality Action Plan will be considered by the Executive and with a recommendation to submit the action plan to Defra for approval.

5.2 Once approved by Defra, the Executive Member, through delegated authority from the Executive, will need to formally

adopt the action plan.

6.0 Air quality work since 2020

6.1 Since 2020, along with the routine monitoring from the NOx tubes and continuous air quality monitor, the council and key partners have continued to work to improve air quality across the district.

Sustainability Supplementary Planning Document

6.2 In March 2021, the council adopted a new Sustainability Supplementary Planning Document (SPD) to provide guidance on the implementation of adopted District Plan (2018) policies related to climate change and sustainable design and construction, to improve the environmental sustainability of new development. The sustainability SPD will be a material consideration in the determination of planning applications and is available on our website - https://www.eastherts.gov.uk/planning-building/planning-policy/supplementary-planning-documents

6.3 The Sustainability SPD has a detailed, 25 page chapter on maximising air quality through the development process. The council's work with the Hertfordshire Climate Change and Sustainability group indicates that the SPD is at the 'leading edge' of planning guidance across the county.

Climate change strategy

6.4 In July 2019, the council unanimously approved a Climate Change Declaration in recognition of the climate emergency we are all facing. This declaration commits the council to take action to address the causes and impacts of climate change across the district. To support the declaration, the council published its Climate Change Strategy 2022-26 and action

plan.

6.5 The Climate Change Strategy lays out how the council, residents, business and other partners can all pull together and help each other make significant and long-lasting improvements to the sustainability of our precious environment, including air quality.

6.6 The strategy and action plan are available on our website - https://www.eastherts.gov.uk/about-east-herts-0/environmental-sustainability/climate-change-strategy-2022-2026

Seeking external funding air quality work

6.7 In July 2022, the government invited local councils across England to bid for funding from a £7 million pot to find innovative ways to improve air quality in their areas. The council submitted a bid to improve knowledge and information about air quality, raise awareness of air pollution as a health issue, and promote alternatives to car travel.

6.8 In February 2023, the council received notification that it has been successful in its bid and had been awarded £126,408 to support this work.

6.9 The proposed project includes direct engagement with community groups, workplaces and schools to highlight steps which individuals can take to reduce air pollution and their exposure to it.

Supporting the switch to e-vehicles

6.10 As part of the council's priority, "sustainability at the heart of everything we do", in December 2022, the council switched its fleet of vehicles from diesel vans to electric cars. This switch

will reduce the council's carbon footprint by nine tonnes per year and will help reduce the impact on air quality from using the vehicles in the town centres and AQMAs.

6.11 The council is finalising a major procurement exercise for the design, supply, implementation and support of e-charging infrastructure in our car parks across the district as well as at village hall and parish council sites in more rural locations.

6.12 The council works closely with Stansted Airport to help the airport reduce the impact of its operations on the air quality in and around Bishop's Stortford. Notably, conditions applied to the approved 2021 planning permission included the installation of rapid electric vehicle charging points at the airport. Stansted is moving forward with the delivery of an EV charging facility at land off Thremhall Avenue, to the south of the airport. It has been designed to allow for the progressive installation of EV chargers as demand increases, as EV ownership increases. The capacity of the site is for approximately 70 vehicles to lay-over at any one time and if required, for each of those spaces to be served by charging infrastructure.

Promoting cycling

6.13 The council is currently working on its Local Cycling and Walking Infrastructure Plan (LCWIP); a transport planning process to identify key networks and concept infrastructure improvements and to prioritise them against set criteria.

6.14 The LCWIP enables a long-term approach to improving local cycling and walking networks and form a vital part of national and local government strategy to increase the number of trips made on foot or by cycle.

6.15 The council is currently at Stage 1 of 6 and determining the scope of the LCWIP. This will be followed by a review of existing routes and gathering information from completed local studies, followed by the development of a draft plan which will be shared with the public for feedback in 2024.

6.16 The final LCWIP will be agreed by both East Herts Council and Hertfordshire County Council in 2024.

6.17 The LCWIP will support a wider project being undertaken by Hertfordshire County Council to create a cycle route which ultimately connects Stansted, Bishop's Stortford, Spellbrook, Sawbridgeworth, the proposed Gilston Garden Villages and Hoddesdon.

6.18 Hertfordshire County Council has already identified a cycle route for the Stansted - Harlow - Lea Valley and prepared concept designs for the length from Bishop's Stortford to Hoddesdon. As well as providing a safe interurban cycle route it will also enable people within these towns and villages to cycle more easily as part of everyday life.

6.19 Relevant County Councillors are being briefed about the designs and the route will be referred to in the forthcoming East Herts Local Cycling and Walking Infrastructure Plan (LCWIP). In due course local people will be invited to shape the proposals further.

Vehicle age and emissions policy for taxis

6.20 Since 2019, the council has had a ground-breaking vehicle age and emissions policy for taxis licensed by East Herts Council. The aim of the policy is to improve air quality in and around the town centres.

6.21 From 01/04/2023 the policy states all taxis which need to be licenced, both new ones and those renewing their licence, must meet the 'Euro 6' emissions standard.

6.22 The council is also currently working with the Hertfordshire Climate Change and Sustainability Partnership (HCCSP) on a county-wide emissions policy which is based on East Herts Council's policy.

Improvements at Stansted Airport

6.23 The council works very closely with the airport in relation to air quality matters and makes representations on all relevant planning applications.

6.24 Of note, the airport is continuing to work with transport operators, local authorities and the Transport Forum as part of the Section 106 commitments to contribute to kick start funding to services and the investment in newer vehicles. By encouraging staff to travel via public transport and improving the service to get to the airport, there is a continued notion that this will result in less traffic using Hockerill Junction.

6.25 Stansted Airport had achieved a public transport mode share of above 51% which is one of the best in the UK and Europe. Some examples of their work, provided by Stansted Airport, include their long-term partnership with Arriva in developing the 510/509/508 services that operate Harlow – Sawbridgeworth – Bishop's Stortford - Stansted Airport. They have grown this service which was an hourly Monday to Saturday services that operated 7am to 7pm, to now operating 24 hours a day, 7 days a week, up to every 12 minutes. They have also contributed to new Euro 6 vehicles. Not only does this provide connections to the airport, but also significantly benefit the local area as provides high frequency, low emissions connections for people connecting between Harlow

and Bishop's Stortford.

6.26 Stansted Airport have also introduced strict criteria for taxis requiring all vehicles to be under three years old.

Promoting air quality to residents

7.1 The council's website has a dedicated air quality page which can be found here - https://www.eastherts.gov.uk/environmental-health/air-quality. The page contains information about air quality and the council's AQMAs as well as links to useful information.

7.2 In addition to the website, the council will use its social media platforms to promote air quality initiatives such as clean air day and successful bids for grant money.

7.3 To help those who may be more susceptible to higher levels of pollution because of respiratory health conditions, the council, along with others in Hertfordshire and Bedfordshire promotes an air pollution alert system which residents can subscribe to via a link on our website. If pollution levels are forecast to be moderate or high, they will receive an alert, so they can plan their day / journey to avoid these areas.

8.0 The impact of development on the AQMAs

8.1 When developing the council's District Plan in 2018, the cumulative impact of development on the allocated sites was investigated. This predicted no undue air quality pressures as a result of the Plan, once factors such as anticipated traffic patterns, improving vehicle emission standards and the likely uptake of alternatives to car use were taken into account.

8.2 Applications for major development across the district, and all development in the AQMAs must submit an air quality

assessment as planning policy expects the applicant to demonstrate how the proposal would have at least a neutral, if not a positive, impact on local air quality. Redesigns and mitigations can be insisted upon as a condition of planning consent in line with both national guidance and the more stringent air quality guidance found in the council's Sustainability Supplementary Planning Document.

8.3 As outlined in paragraph 10.5 below, the levels of pollution around the Hockerill junction in Bishop's Stortford (our second AQMA), have continued to decrease, despite the increased development in and around Bishop's Stortford.

8.4 Members will also note that through the council's District Plan we are not only addressing air pollution through good quality infrastructure, public transport and encouraging people to walk and cycle rather than drive, we are also helping people to become fitter and healthier.

9.0 Use of 'Section 106' financial contributions

9.1 Planning obligations under Section 106 of the Town and Country Planning Act 1990 (as amended), commonly known as 'Section 106' agreements, are a mechanism which make a development proposal acceptable in planning terms, that would not otherwise be acceptable. They are focused on site specific mitigation of the impact of development. Section106 agreements are often referred to as 'developer contributions' along with highway contributions and the Community Infrastructure Levy.

9.2 Where appropriate the council will seek Section 106 financial contributions from developers to help mitigate the impact of any development or require specific infrastructure to be provided as part of the development.

9.3 As part of the Bishop's Stortford North development, the developer will pay £20,000 towards monitoring and mitigation measures in Bishop's Stortford. This is payable prior to the occupation of the 1,000th dwelling, which is anticipated in early 2024. This funding will feed directly into the new Air Quality Action Plan.

9.4 Other Section 106 financial contributions have been earmarked for projects such as new pathways and cycle route from Bishop's Stortford North to the town centre via Castle Park.

9.5 Section 106 financial contributions relating to sustainable transport, have been identified and are collected and allocated by Hertfordshire County Council.

9.6 Further Section 106 final contributions are expected from the Harlow and Gilston Garden Town development which was considered by the Development Management Committee at the end of February 2023.

10.0 Current state of play

10.1 Aside from the obvious and devastating health impacts of the COVID Pandemic, there was a significant change to the way people work during this time. The lockdowns and restrictions on movement saw an increase in home-working and thereby decrease in traffic. This renders any monitoring data for this period relatively useless when monitoring long-term trends.

10.2 In the year following the lifting of the pandemic restrictions, as people settle into new working practices, the monitoring data is also unreliable for making any long-term predictions on the future of the AQMAs.

10.3 Data we obtain from the 2022 monitoring will be important in showing us the impact of everyone's new working arrangements (largely working from home). This data is likely to be available late summer 2023.

10.4 Air quality data for 2017-2021 can be found in **Appendix A, B and C** to this report. In should be noted that to revoke an AQMA, the council needs three years or more data showing NO_2 levels consistently below 36 ug/m^3, that is, there is consistent record of air pollution being at least 10% *below* the national objective of 40 ug/m^3. Although emissions have continued to drop during the pandemic, it is prudent to assess whether lower levels pertain *after* pandemic before seeking to revoke an AQMA.

Air quality in Bishop's Stortford AQMA

10.5 From the data in Appendix A, members will note that of the four main junctions, one (Stansted Road) has been consistently below the national Air Quality Objective of 40 ug/m^3 since 2017, with Hockerill Street also fluctuating just above and below the national Air Quality Objective.

10.6 From the source apportionment undertaken by Bureau Veritas, we believe the main contributor is diesel passenger cars.

10.7 Hertfordshire County Council have also recently announced that because of significant abuse of traffic regulations in Bishop's Stortford causing clogging of the junctions and unnecessary congestion, they will be applying for legal powers for cameras to monitor motorists turning left or right out of Adderley Road into The Causeway in Bishop's Stortford for "moving traffic offences". It will be the first location in Hertfordshire to be the subject of "unattended camera

enforcement" under the powers.

Air quality in Hertford's AQMA

10.8 From the data in **Appendix B** members will note four of the six NOx tube monitoring sites have been consistently below the National Air Quality Objective of 40 ug/m^3 since 2017.

10.9 It is likely that improving emission levels from cars, changes to commuting patterns due to the pandemic and efforts to making greener travel without using a car (for example, the improvements the pedestrian underpasses under Gascoyne Way) have all contributed to the drops in air pollution.

10.10 Once NO_2 readings following the pandemic are available, the case for revoking this AQMA will be considered in line with the requirements set out in paragraph 10.4 above.

Air Quality in Sawbridgeworth's AQMA

10.11 From the data in Appendix C, members will note that the NO_2 levels have been gradually falling since 2016, with levels along parts of London Road now below the National Air Quality Objective of 40 ug/m^3 in around 2018.

11.0 Conclusion

11.1 To conclude, the council has and continues to work with key partners to undertake a wide range of activities aimed at improving air quality. Additionally, where the opportunity arises, the council will aim to bid for external funding to support this work.

11.2 With regards to the question from members as to whether the air quality action plan is being followed and is it fit for purpose, members will note from the information in Sections

4.0, 5.0 and 6.0 above that the air quality action plan is currently being refreshed and during this interim period, the council continues to strive to improve air quality across East Herts.

11.3 With regards to the question from members as to whether our website is advertising the issues sufficiently to our residents Section 7.0 above outlines how the council uses the website and social media platforms to promote air quality.

11.4 With regards to the question from members as to whether we are fulfilling our statutory duties, members will note from the report that our statutory duty with regards to air quality and AQMAs is being fulfilled through the production of an air quality action plan and the wide range of activities being undertaken by the council and key partners.

11.5 With regards to the question from members as to whether the new housing developments have had a negative impact on the existing AQMAs, Section 8.0 above outlines the council's assessment of this and evidence from Bishop's Stortford's AQMA which supports this position.

11.6 With regards to the question from members as to whether 'Section 106' financial contributions coming from developments have been used as they should have been with regards to air quality, Section 9.0 above sets out the position that, where possible, Section 106 financial contributions are being used to improve air quality.

12.0 Reason(s)

12.1 Given the salience of sustainability in the council's Corporate Plan and the potential health impacts of poor air quality, it is appropriate and timely for the Overview and Scrutiny Committee to review the work guided and overseen by the

Executive Member for Environmental Sustainability regarding air quality.

13.0 Options

13.1 Within the context of continuing financial pressures on the council, scale back or cease work on air quality – NOT RECOMMENDED as the declaration of AQMAs requires the council to work with partners to reduce pollution levels. Arguably, only continued work to produce a refreshed Air Quality Action Plan and seek external funding for projects will enable the council to play its part, alongside Hertfordshire County Council, national government and local communities and people, will enable the council to build on the air quality gains seen to date. A corollary of this is that there would be little in future for the Overview and Scrutiny Committee to consider.

13.2 Continue with ad hoc work on air quality without renewing the Air Quality Action Plan – NOT RECOMMENDED as although this approach would likely see some benefits, the opportunities for joined-up working and the bringing together of actions could be lost. The Overview and Scrutiny Committee could continue to review actions from time-to-time.

13.3 Refresh the Air Quality Action Plan as discussed in this report and continue with joined-up actions – RECOMMENDED. The Overview and Scrutiny Committee could consider progress on a periodic basis.

14.0 Risks

14.1 There is a risk to health from inaction on air pollution in the district.

14.2 There is a reputation risk to the council if it were considered not to be taking the problem of air pollution seriously.

14.3 There is a financial risk as failure to work with all interested parties and communities on the prevention of air pollution could ultimately led to higher cost interventions, such as road closures, road pricing and the like, being required to reduce air pollution.

Implications/Consultations

Community Safety
No

Data Protection
No

Equalities
Yes – Poor air quality can disproportionately impact people with particularly protected characteristics, notably disabled people with long-term health conditions such as asthma and chronic obstructive pulmonary disease (COPD) and older people who are more likely to have such disabilities.

Environmental Sustainability
Yes – The work identified in this report will improve environmental sustainability.

Financial
No

Health and Safety
No

Human Resources
No

Human Rights
No

Legal
The declaration of AQMAs requires the council to work with partners to reduce pollution levels.

Specific Wards
No

Background papers, appendices and other relevant material

16.1 Background Information:

16.2 Appendices

Appendix A – NO_2 levels at Hockerill Junction, Bishop's Stortford Air Quality Management Area

Appendix B – NO_2 levels Gascoyne Way, Hertford Air Quality Management Area

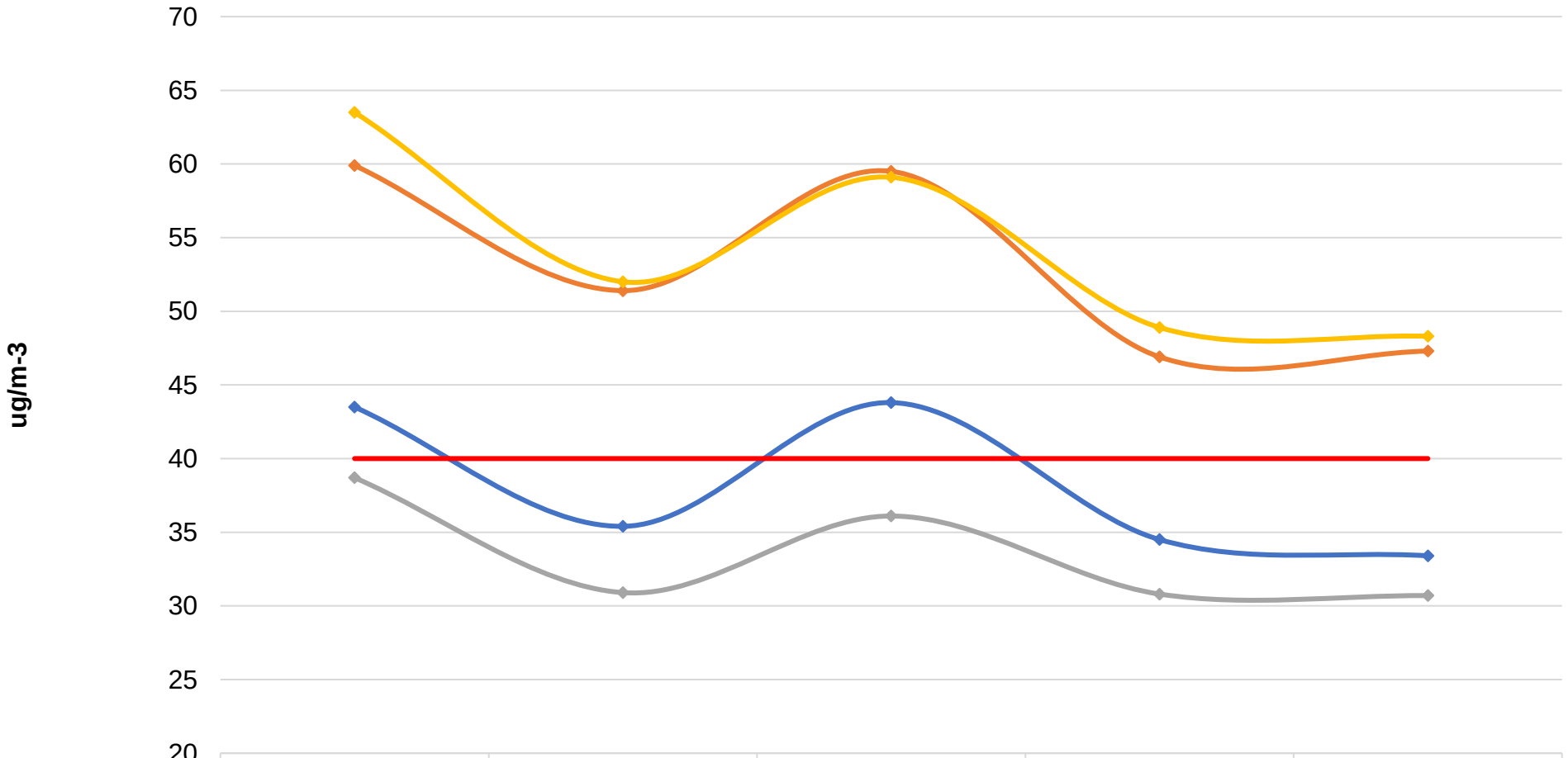
Appendix C – NO_2 levels London Road, Sawbridgeworth Air Quality Management Area

Contact Member
Councillor Graham McAndrew, Executive Member for Environmental Sustainability. graham.mcandrew@eastherts.gov.uk

Contact Officer
Jonathan Geall, Head of Housing and Health, Tel: 01992 531594
jonathan.geall@eastherts.gov.uk

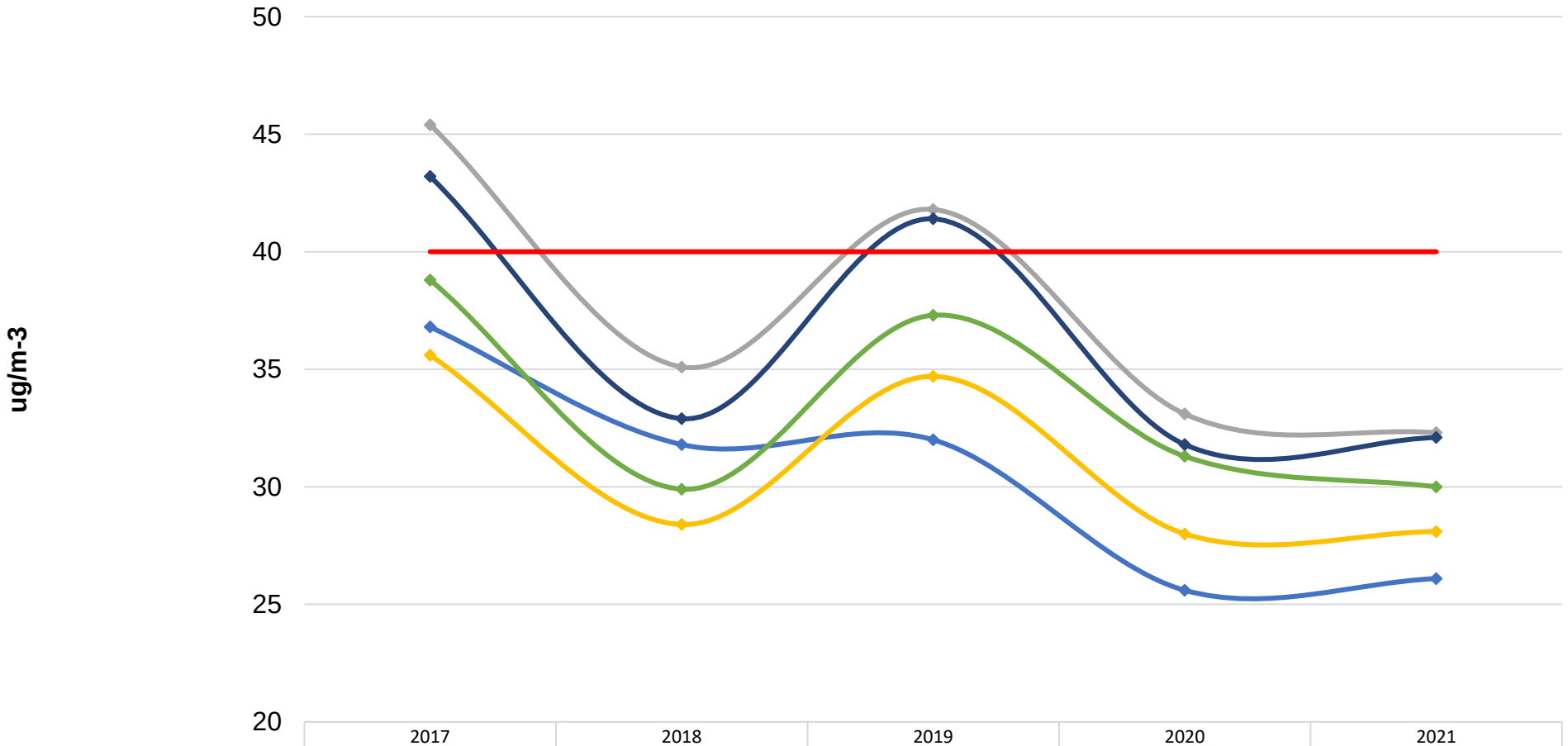
Report Author
Paul Thomas-Jones, Service Manager (Environmental Health), Tel: 01992 531491. paul.thomas-jones@eastherts.gov.uk

NO2 Levels at Hockerill Junction
Bishop's Stortford Air Quality Management Area



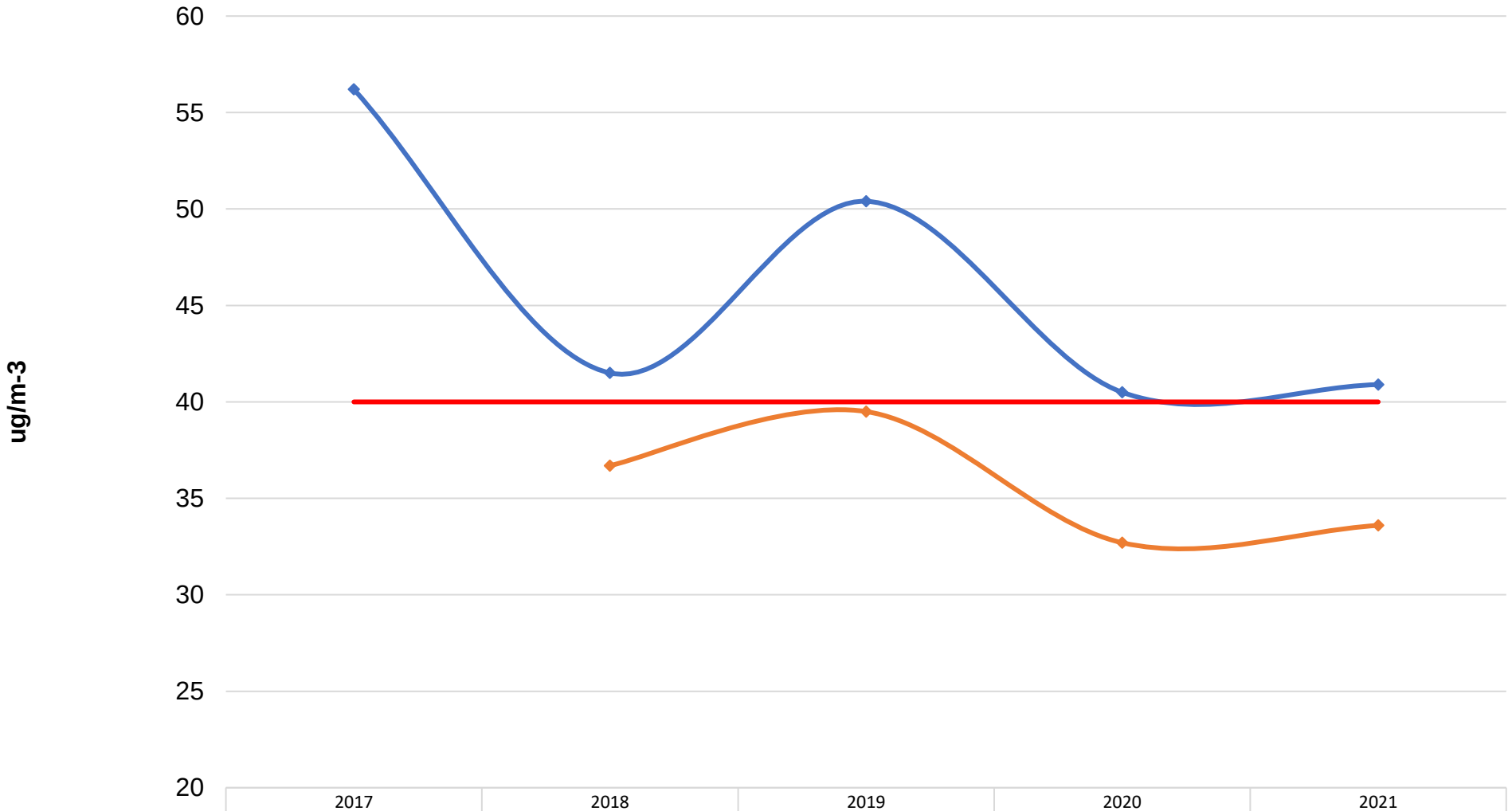
	2017	2018	2019	2020	2021
Hockerill Street	43.5	35.4	43.8	34.5	33.4
Dunmow Road	59.9	51.4	59.5	46.9	47.3
Stansted Road	38.7	30.9	36.1	30.8	30.7
London Road	63.5	52	59.1	48.9	48.3
National Objective	40	40	40	40	40

NO2 Levels Gascoyne Way
Hertford Air Quality Management Area



	2017	2018	2019	2020	2021
EH79/80/81 - Gascoyne Way	36.8	31.8	32	25.6	26.1
EH25 - Old Cross	45.4	35.1	41.8	33.1	32.3
EH28/48/49 - Castle Street	35.6	28.4	34.7	28	28.1
EH30 - Hertingfordbury Road	38.8	29.9	37.3	31.3	30
EH42/43/44 - West Street	43.2	32.9	41.4	31.8	32.1
National Objective	40	40	40	40	40

NO2 Levels London Road
Sawbridgeworth Air Quality Management Area



	2017	2018	2019	2020	2021
EH57 - Bell Street	56.2	41.5	50.4	40.5	40.9
EH91 - London Road		36.7	39.5	32.7	33.6
National Objective	40	40	40	40	40

East Herts Council

Overview and Scrutiny Committee

Date of Meeting: **21 March 2023**

Report by: **James Ellis, Head of Legal and Democratic Services**

Report title: **Regulation of Investigatory Powers Act (RIPA) Policy Review**

Ward(s) affected: **All**

Summary

- This report updates the Committee on the Council's recent IPCO inspection and seeks to implement recommended changes to the RIPA policy.

RECOMMENDATIONS FOR OVERVIEW AND SCRUTINY:

(A) The Committee considers the content of the report and provides any observations to the Head of Legal and Democratic Services.

(B) The revised Regulation of Investigatory Powers Act (RIPA) Policy be sent for adoption by the Executive.

1.0 Proposal(s)

1.1 To implement changes to the Council's RIPA Policy as suggested in the IPCO inspection report.

2.0 Background

2.1 The Investigatory Powers Commissioner's Office (IPCO)

oversee the Council's use of investigatory powers, ensuring that they're used in accordance with the law and in the public interest. They do this by inspecting the Council on a three-yearly basis.

2.2 The Council was last inspected in 2019, meaning that the next scheduled inspection was due in 2022.

2.3 This inspection by the IPCO took place on 27th October 2022, with the resultant Inspection Report being provided to the Chief Executive on 16th November 2022.

2.4 The report was both positive and complimentary of the changes implemented by the Council since the last inspection in 2019, saying:

"*The information provided has demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection. [The Inspector] identified significant improvements since the previous inspection in 2019, and I am pleased to hear that all the action points arising from that earlier inspection have now been discharged… your Council is in a much stronger position should the need to exercise the powers arise*.

2.5 The inspector did, however, make some suggested amendments to the Council's RIPA Policy in order to address some recent changes pertaining to Communications Data in the Investigatory Powers Act, as well as some additional changes to how information on social media was to be treated.

2.6 The changes are shown in track changes at Appendix A, with a clean version available at **Appendix B**.

3.0 Reason(s)

3.1 Whilst the Council does not actively make use of its RIPA powers, it is important that RIPA, the policy and its usage, or

otherwise, are kept at the forefront of Members' minds.

3.2 Updating the policy to reflect the recommendations by the IPCO displays that the Council is has taken heed of the advice and it actively taking steps to make sure its policy is fit for purpose.

4.0 Options

4.1 To not implement the IPCO's recommended changes to the policy, this is NOT RECOMMENDED as to do so would inevitably lead to the policy becoming out of date and place the Council in a position where it was not meeting its legal obligations.

5.0 Risks

5.1 It is important that the Council continues to operate in accordance with RIPA to ensure that it is able to effectively manage its reputational risk whilst also exercising its legitimate evidence gathering powers in connection with enforcement activity.

6.0 Implications/Consultations

6.1 Not regularly reporting on the Council's use of RIPA would risk it slipping out of the consciousness of Members.

Community Safety
Yes – Allows the Council to legal make use of investigatory practices governed by RIPA, which could be utilised to protect communities from illegal activities.

Data Protection
No

Equalities
Yes - No RIPA investigations have been conducted by the council and so there is no data against which to assess the potential equalities aspects of RIPA use. If the council sought to use RIPA powers at some point, the equalities aspects would be considered at that time.
The risk of having a policy that is not fit-for-purpose could lead to unintended equalities issues or risk of the perception of this.

Environmental Sustainability
No

Financial
No

Health and Safety
No

Human Resources
No

Human Rights
Yes – The use of powers under RIPA directly affects a person's right to respect for private and family life under Art 8 of the Human Rights Act. It is imperative that RIPA is utilised correctly so as to make legal those potential intrusions.

Legal
Yes – The Regulation of Investigatory Powers Act 2000 ("RIPA") enables local authorities to carry out certain types of surveillance activity, as long as specified procedures are followed. The information obtained as a result of surveillance operations can be relied upon in court proceedings providing RIPA is complied with. The Investigatory Powers Act 2016 ("IPA") is the main legislation governing the acquisition of communications data. The information obtained as a result of these acquisitions can also be relied upon in court proceedings providing IPA is complied with. Full details of the

RIPA requirements and compliance are set out in the Policy, with relevant documents and guidance document available to relevant officers via the intranet should they consider it necessary to use these powers.

Specific Wards
No

7.0 Background papers, appendices and other relevant material

7.1 **Appendix A** – Updated RIPA Policy with track changes.

7.2 **Appendix B** – Clean version of the updated RIPA Policy.

Contact Member
Councillor George Cutting, Executive Member for Corporate Services
george.cutting@eastherts.gov.uk

Contact Officer
James Ellis, Head of Legal and Democratic Services, Tel: 01279 502170
james.ellis@eastherts.gov.uk

Report Author
James Ellis, Head of Legal and Democratic Services, Tel: 01279 502170
james.ellis@eastherts.gov.uk

Appendix A

Style Definition: TOC 2: Indent: Left: 0.39 cm, Hanging: 1.11 cm

Style Definition: TOC 1: Font: Bold, Indent: Left: 0.25 cm

East Herts District Council

Regulation of Investigatory Powers Act 2000

Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Regulation of Investigatory Powers Act 2000 Policy
Author – name and title	James Ellis, Head of Legal & Democratic Services
Owner – name and title	James Ellis, Head of Legal & Democratic Services
Date	~~June~~ March 2023~~2~~
Approvals	Executive
Version	2.0~~1.1~~
Next Review Date	June 2024~~3~~

East Herts Council

Regulation of Investigatory Powers Act 2000
Policy

Contents

1. Introduction

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ("RIPA") came into force on 25 September 2000 and sought to regulate covert investigation practices undertaken by a number of bodies, including local authorities.

This Policy is the framework on which East Herts Council ("the Council") applies the provisions of RIPA as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by the Investigatory Powers Commissioner's Office (the "IPCO") (formerly the Office of Surveillance Commissioners – OSC) and individual Services to deal with the specific issues of their service.

1.2 Background

The Human Rights Act 1998 requires the Council to have respect for the private and family life of citizens. However in rare cases, it may be lawful, necessary and proportionate for the Council to act covertly in ways that may interfere with an individual's rights.

The rights conferred by Article 8 of the Human Rights Act are not absolute rights, but qualified right, meaning that it is still possible for a public authority to interfere with those rights provided the following criteria are satisfied;

(a) It is done in accordance with the law
(b) It is necessary (as defined in this document); and
(c) It is proportionate (as defined in this document).

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

It is possible that unauthorised surveillance will be a breach of a person's right to privacy under Article 8. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not

obtained, the surveillance carried out will not have the protection that RIPA affords.

If the correct procedures are not followed;

- evidence may be disallowed by the courts,
- a complaint of maladministration could be made to the Ombudsman, and/or
- the Council could be ordered to pay compensation

It is therefore essential that this document, along with any further guidance that may be issued from time to time by the Head of Legal and Democratic Services, always be complied with.

1.3 Policy Review

RIPA and this document are essential for the effective, efficient and legal operation of the Council's covert surveillance activity. This document will, therefore be kept under annual review by the Head of Legal and Democratic Services.

Authorising Officers, as defined below, must bring any suggestions for the continuous improvement of this document to the attention of the Head of Legal and Democratic Services, at the earliest possible opportunity.

1.4 Scope

RIPA does not;

- Make unlawful anything that is otherwise lawful
- Impose any new statutory duties, or
- Prejudice or disapply any existing powers available to the Council to obtain information by any means not involving conduct that is governed by RIPA. (For example it does not affect the Council's current powers to obtain information from the DVLA or the Land Registry).

If RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, Employment Tribunal hearings and a complaint to either the Local Government Ombudsman or the

Investigatory Powers Tribunal. It therefore provides protection both for the Council and any officer who may have been involved in an investigation.

It should also be noted that the requirements of RIPA, and this policy, extends to external agencies working on behalf of the Council. Where such agencies are carrying out the Authority's statutory functions, the Authority remains liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so.

RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

- The use of Directed Surveillance
- The Use of Covert Human Intelligence Sources
- The Acquisition and Disclosure of Communications Data

2. Definition of Surveillance

"Surveillance" includes:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations or their other activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by, or with, the assistance of a surveillance device, which will include cameras, video, and listening or recording devices.

Surveillance can be either overt or covert.

2.1 Overt Surveillance

The overwhelming majority of surveillance undertaken by the Council will be done overtly, meaning there will be nothing secretive or hidden about the way it is conducted. In many cases officers will be going about Council business openly (e.g. a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if it continues.)

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 Head of Legal and Democratic Service or the Senior Responsible Officer

Use of body worn cameras should also be overt. Badges should be worn by officers stating body cameras are in use and it should be announced verbally that recording is taking place. In addition, cameras should only be switched on when recording is necessary e.g. when issuing parking tickets.

2.2 Covert Surveillance

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

3. Directed and Intrusive Surveillance

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
c) 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 RIPA to be sought for the carrying out of the surveillance.

3.2 Intrusive Surveillance

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

Surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or
b) where a device placed outside consistently provides information of the same or equivalent quality and detail as might be expected if it were in the premises or vehicle, or
c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device **OR** when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

A private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the council has no statutory powers to interfere with private property.

4. Identifying directed surveillance

You should ask yourself the following questions:

4.1 Is the surveillance overt or covert?

Refer to paragraphs 2.1 and 2.2 above. If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. If the proposed surveillance is covert in nature, then refer to paragraph 4.2 below.

4.2 Can the same outcome be achieved by overt means?

Does the surveillance have to be covert? If not, then you should proceed with overt surveillance, including the use of signs and other notification techniques so that the subject of the surveillance is aware it is taking place.

4.3 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.4 Is the surveillance likely to result in the obtaining of private information about a person?

Private information is defined in RIPA section 26 (10) as including any information relating to a person's private or family life.

The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8.

The Article also protects a right to identity and personal development and includes an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.5 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, an environmental crime officer would not require an authorisation to conceal themselves and observe a suspicious person which they came across in the course of a routine patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. Covert Human Intelligence Sources (CHIS)

A person is a covert human intelligence source ("CHIS") if;

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship if, and only if, the relationship is conducted in a

manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly if, and only if, it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

A member of the public who volunteers information to the Council is not a covert human intelligence source.

Likewise, members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS either as they are not usually required to establish or maintain a covert relationship.

It should be noted, however, that if the information provided is recorded as potentially useful or actionable, there is potential duty of care to the individual and the onus is on the public authority to manage human sources properly. Authorising Officers should be alive to the possibility of 'status drift'. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

5.1 Conduct and use

The conduct or use of CHIS must be authorised in accordance with RIPA.

Conduct of a CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information.

Use of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

The use of a juvenile CHIS may only be authorised for ~~one~~ four months at a time[1].

[1] Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018/715

5.2 Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert 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).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, or an adult is observing a juvenile test purchase, this will require authorisation, as directed surveillance. In all cases, a prior risk assessment is essential in relation to any young person used for a test purchase.

5.3 Security and Welfare

Only the Chief Executive is able to authorise the use of vulnerable individuals and juvenile CHIS's. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the Covert Human Intelligence Source Code of Practice which can be found here.

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

5.4 Criminal Conduct Authorisations

The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 (CHIS(CC)A) received Royal Assent on 1 March 2021 and went live for the police on 15 September 2021. CHIS(CC)A amends the Regulation of

Investigatory Powers Act 2000 and provides an express power to authorise a CHIS to participate in conduct which would otherwise constitute a criminal offence. This power is known as a Criminal Conduct Authorisation (CCA). It is important to note that local authorities have not been given these powers and it is mentioned here for the avoidance of doubt.

6. Communications Data

Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer.

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this 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 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

Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold

- an offence which involves, as an integral part of it, the sending of a communication or breach of a person's privacy.

Further guidance can be found in paragraphs 3.3 to 3.13 of the communications data Code of Practice.

The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through National Anti-Fraud Network (NAFN) and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the Communications Data Code of Practice).

~~The powers contained in Part 1 of Chapter 2 of RIPA permit Local Authorities to obtain information relating to the use of a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of e-mails or interaction with websites.~~
~~Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.~~

~~Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information~~

~~A third type of data (Traffic data) is not accessible to local authorities.~~

~~6.1 Customer data – (Subscriber data, RIPA s21(4))~~

~~Customer data is the most basic. It is data about users of communication services. This data includes:~~

- ~~Name of subscriber~~
- ~~Addresses for billing, delivery, installation~~
- ~~Contact telephone number(s)~~

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Normal

Formatted: Hyperlink, Font: (Default) +Body (Calibri), 11 pt, Not Bold, Font color: Auto

Formatted: Hyperlink, Font: (Default) +Body (Calibri), 11 pt, Not Bold, Font color: Auto

Formatted: Hyperlink, Font: (Default) +Body (Calibri), 11 pt, Not Bold, Font color: Auto

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

6.2 Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e- top up details

6.3 Traffic data – (Traffic data, RIPA s21(6))

In relation to communications means:

- any data identifying or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted
- any data identifying or selecting or purporting to identify or select apparatus through which, or by means of which the communication is or may be transmitted

any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the

~~transmission of any communication aany data identifying the data or other data as data comprised in or attached to a particular communication but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.~~

7. RIPA Authorisation Procedure

7.1 General

Directed surveillance~~,~~ and the use of CHIS ~~and the acquisition of communications data~~ must be lawfully carried out in strict accordance with the terms of the relevant authorisation and Magistrates Court approval.

The Council can only authorise directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:

a) S146 of the Licensing Act 2003 (sale of alcohol to children);
b) S147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
c) S147A of the Licensing Act 2003 (persistently selling alcohol to children); and
d) S7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under the age of 18)

The Council will only very rarely make use of CHIS so the applicant officer should consult the Head of Legal and Democratic Services before making an application for a CHIS authorisation in order to ensure that the current statutory requirements and best practice are being observed.

Applications for authorisations and notices requesting communications data must be processed through the Council's Home Office accredited single point of contact ("SPoC"). As the need to obtain such information will only very occasionally arise the applicant officer should contact the Head of Legal and Democratic Services before making an application in order to ensure that current statutory requirements and best practice are being observed.

All applications for authorisation must be sought and granted before any surveillance activity takes place. The decision whether or not to authorise an application must not be taken with the benefit of hindsight. This should be borne in mind when submitting an application to the Magistrates' Court.

Once approved, the original authorisation and accompanying paperwork must be forwarded to the RIPA Co-Ordinator (Senior Solicitor – Corporate Legal Team) to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the central register.

7.2 Before Making the Application

Before making an application for an authorisation, the requesting officer must;

- read this policy document,
- determine whether the activity that they are proposing to conduct involves directed surveillance or the use of a CHIS,
- assess whether the activity will be in accordance with the law – is it governed by RIPA,
- assess whether the activity is necessary and why,
- assess whether the activity is proportionate.

If the activity can be conducted overtly or if a less intrusive option is available and practical, then that option should be pursued rather than obtaining a RIPA authorisation.

7.3 Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved.

Confidential information consists of personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Head of Legal and Democratic Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's spiritual welfare or matters of medical or journalistic confidentiality.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act 2000.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive or, in his absence, the person acting as the Head of Paid Service.

7.43 Who can give ~~Provisional~~ Authorisations?

Authorisations may only be given by the Authorising Officers listed in Appendix B. Only the Chief Executive can authorise the use of a CHIS, or the acquisition of confidential information (see paragraph 7.3 above).

Applications for the acquisition of Communications data can only be issued by a Home Office accredited single point of contact ("SPoC") (see paragraph 7.8 below)

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Head of Legal and Democratic Services before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training or a one-to-one meeting with the Head of Legal and Democratic Services, on such matters, will be kept by the Head of Legal and Democratic Services.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. Where an Authorising Officer authorises such an investigation or operation the central register will highlight this and the Commissioner or inspector will be notified of this during his or her next inspection

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of authorisations and associated documentation to the Head of Legal and Democratic Services, that these are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

7.54 Grounds for Authorisation

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant an ~~provisional~~ authorisation for the carrying out of directed surveillance or for the use of a CHIS or for the obtaining or disclosing of communications data unless they have given **personal consideration** to the facts and believes:

a) that an ~~provisional~~ authorisation is necessary, and
b) the ~~provisionally~~ authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, ~~provisional~~ authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Authorisation cannot be sought, and authority must not be given unless you are satisfied that the surveillance is "**proportionate**." You have to make sure that any interference with privacy is justified by the end being sought. Unless the benefit to be obtained from surveillance is significant, and unless the problem you are seeking to tackle is serious, the use of surveillance is unlikely to be proportionate.

The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and other minor offences will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities.

Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

7.~~6~~5 Collateral Intrusion

Before ~~provisionally~~ authorising an investigation, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation; known as collateral intrusion. The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for an ~~provisional~~ authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

7.~~7~~6 Judicial Approval

The Council is only able to grant an ~~provisional~~ authorisation or renewal to conduct covert surveillance. No ~~provisional~~ authorisations, nor any surveillance granted under them, will take effect until judicial approval has been sought and granted by a Magistrates' Court.

Once the authorising officer has authorised the directed surveillance or CHIS, the investigating officer who completed the application form should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The investigating officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition the investigating officer will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the investigating officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate.

The Justice of the Peace will also consider whether there continues to be reasonable grounds.

The Justice of the Peace must also be satisfied that the person who granted the authorisation was an appropriate designated person and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for directed surveillance has been met.

The Justice of the Peace will record his/her decision on the order section of the judicial application/order form.
A copy of the RIPA form and judicial application/order form will be retained by the Court.

If the authorisation is approved the council may commence the activity.
If the Justice of the Peace refuses to approve the authorisation the council may not commence the activity although, if the reason for refusal is a technical error, the council may address this and reapply without going through the internal authorisation process again.

The Justice of the Peace may refuse to approve the authorisation, and quash it. The exercise of this power should not take place until the applicant has at least two business days from the date of the refusal to make representations.

7.87 ~~Provisional~~ Authorisation for Communication Data

The Act provides two different ways of ~~provisionally~~ authorising access to communications data; through an ~~provisional~~ authorisation under Section 22(3) and by a provisional notice under Section 22(4).

An ~~provisional~~ authorisation would, following judicial approval, allow the authority to collect or retrieve the data itself. A provisional notice is given

to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An Authorising Officer decides whether or not an ~~provisional~~ authorisation should be granted, or a provisional notice given.

An ~~provisional~~ authorisation under Section 22(3) may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

Notices and, where appropriate, ~~provisional~~ authorisations for communications data must be channelled through SPoC's. The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

The Council use the services of the National Anti-Fraud Network (NAFN) for all Communications Data enquiries and as such NAFN performs the role of a SPoC through their qualified SPoC officers. All applicants must be registered with NAFN via the NAFN website at www.nafn.gov.uk

Applications to obtain communications data should be made on the NAFN standard form available on the NAFN website and submitted in the first instance to the SPoC. If appropriate the SPoC will forward the application to a Council Authorising Officer for either the ~~provisional~~ authorisation of conduct or the ~~provisional~~ issuing of a notice.

If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will return the ~~provisional~~ authorisation or notice to the SPoC who will then liaise with the applicant and the postal/telecommunications company, after the appropriate Judicial Approval has been obtained. The disclosure of data under a notice will only be made to the Authorising Officer.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection

Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

8. Activities by other public authorities

The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9. Joint Investigations

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

a) wishes to use the Council's resources (e.g. CCTV), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources
b) wishes to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

10. Duration, reviews, renewals and cancellation of authorisations

10.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source
b) three months from the date of judicial approval for directed surveillance
~~c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.~~

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

10.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations.

Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

10.3 Renewals

If at any time before an authorisation ceases to have effect, it is necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 calendar months, beginning with the day when the original authorisation would have expired. Magistrates Court approval is required before a renewal takes effect.

Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation and are approved by the Magistrates' Court. The renewal should be kept/recorded as part of the central record of authorisations.

The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

Authorisations can be renewed in writing shortly before the maximum period has expired. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

An authorisation cannot be renewed after it has expired.

A further requirement in relation to renewal of a CHIS is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source

For the purposes of making an Order, the Magistrates have considered the results of that review.

10.4 Cancellations

The Authorising Officer must cancel an authorisation if they become satisfied that the surveillance is no longer required or appropriate.

Authorisations should not be allowed simply to lapse. The duty to cancel a notice falls on the Authorising Officer who issued it.

The Authorising Officer must then cancel the Application without delay. When cancelling the authorisation the Authorising Officer is required to consider whether the surveillance was effective, necessary and met its objectives. Cancellations must be made using the cancellation form and should briefly detail what product(s) resulted from the surveillance.

When cancelling an authorisation, the Authorising Officer must ascertain what recorded material has been obtained by the use of directed surveillance. The Authorising Officer should comment on the recorded material and how it is to be managed or used thereafter. If the matter is not proceeding to a prosecution, the Authorising Officer must be satisfied that any recorded material has been securely destroyed.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

11. Record Management

11.1 Central record of all Authorisations

The Head of Legal and Democratic Services shall hold and monitor a centrally retrievable record of all ~~provisional and~~ judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Head of Legal and Democratic Services to ensure that the records are regularly updated.

The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The Head of Legal and Democratic Services will monitor the submission of ~~provisional and~~ judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Head of Legal and Democratic Services, shall contain the following information:

a) the type of authorisation or notice
b) the date the ~~provisional~~ authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;
e) the unique reference number (URN) of the investigation or operation;

f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) the date the authorisation or notice was cancelled.

11.2 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and ~~provisional~~ authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;
b) a record of the period over which the surveillance has taken place;
c) the frequency of reviews prescribed by the Authorising Officer;
d) a record of the result of each review of the authorisation or notice;
e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;
f) the date and time when any instruction was given by the Authorising Officer,
g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

11.3 Records relating to a CHIS

Proper records must be kept of the authorisation and use of a CHIS. An Authorising Officer must not ~~grant~~ agree an ~~provisional~~ authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person

with the responsibility for maintaining a record of the use made of the CHIS.

The records shall contain the following information:

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant investigating authority other than the Council;
d) the means by which the source is referred to within each relevant investigating authority;
e) any other significant information connected with the security and welfare of the source;
f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g) the date when, and the circumstances in which, the source was recruited;
h) the identities of the persons who, in relation to the source;
    i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare
    ii. have a general oversight of the use made of the source (not to be the person identified in h) i.
    iii. have responsibility for maintaining a record of the use made of the source
i) the periods during which those persons have discharged those responsibilities;
j) the tasks given to the source and the demands made of him in relation to his activities as a source;
k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l) the information obtained by the conduct or use of the source;
m) any dissemination of information obtained in that way; and
n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Records which reveal the name(s) of the CHIS should only be disclosed to persons to the extent that there is a need for access to them; if legally necessary; or if ordered by any Court.

12. Retention and destruction

Formatted: Font: (Default) Open Sans, 12 pt, Bold, Font color: Black

Formatted: Normal, Indent: Left: 0 cm

Generally, all material (in whatever media) produced or obtained during the course of investigations subject to RIPA authorisation should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) ~~(EU) 2016/679~~, the Freedom of Information Act 2000 and any other legal requirements, including those of confidentiality and the Council's policies and procedures regarding document retention.

Material obtained from properly authorised surveillance or a CHIS may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a CHIS or the obtaining or disclosure of communications data.

RIPA surveillance and CHIS records must be available for inspection by the Investigatory Powers Commissioner and retained for at least five years. Information obtained through covert surveillance or CHIS activity, and all copies, extracts and summaries which contain such material, should also be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out in section 9.5 of the Covert Surveillance and Property Interference Code of Practice.

If such information is retained, it should be reviewed at appropriate intervals in line with the relevant retention schedules to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material and the authorising officer, (in consultation with the SRO, is responsible for the retention / destruction decisions in connection with covertly acquired material.

Formatted: Font: (Default) Open Sans, 12 pt, Font color: Black

13. Social Media Sites

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).

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 i.e. where privacy setting are available, but not applied, 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, 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 privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of 'open source' sites, however, may constitute directed surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance~~.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of any relevant guidance and the Council's separate policy regarding the use of **Social Networking Sites and Conduct of Investigations**.

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'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 engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an

investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

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.

As set out 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.'

14. Scrutiny of investigatory bodies

The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it.

The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at https://www.ipco.org.uk/

15. Elected Members

The elected members of the Council will review the council's use of RIPA and the authority's policy and guidance documents at least once a year. They will also be kept informed on a quarterly basis to ensure that it is being used consistently with the council's policy and that the policy remains fit for purpose. Members will not, however, be involved in making decisions on specific authorisations.

Formatted: Font: (Default) Open Sans, 12 pt, Font color: Black

Formatted: Normal, Indent: Left: 0 cm

Formatted: Font: (Default) Open Sans, 12 pt, Font color: Black

Formatted: Normal, Indent: Left: 0 cm

Formatted: Font: (Default) Open Sans, 12 pt, Font color: Black

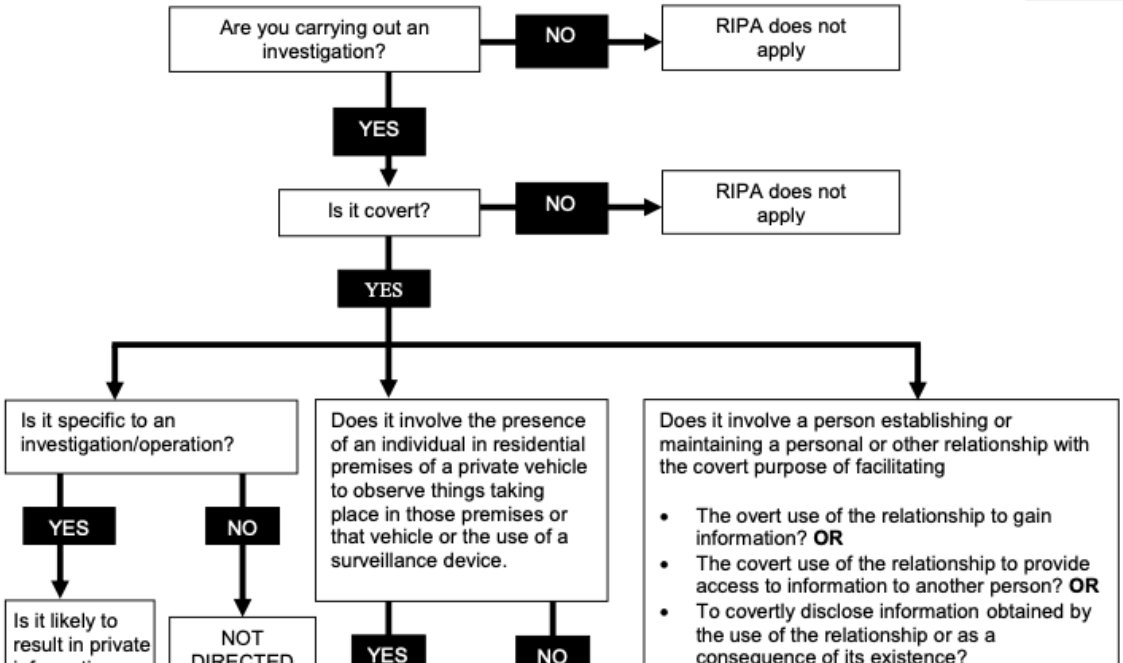
Formatted: Normal, Indent: Left: 0 cm

APPENDIX A

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000

Do you need Authorisation?



APPENDIX B

List of Authorised and Responsible Officers

RIPA Authorising Officers	Chief Executive, Deputy Chief Executive, Head of Operations, Head of Housing and Health Head of Planning
Authorising operations where confidential information may be obtained	Chief Executive only
CHIS Authorising Officer	Chief Executive only

CHIS Controller/Handler	Head of Operations Head of Housing and Health Head of Planning
Senior Responsible Officer	Head of Legal and Democratic Services

Please note:

- Where use of a CHIS is authorised, the head of the directorate carrying out the activity shall usually act as the CHIS Handler, with the CHIS Controller role being allocated by the Chief Executive.
- Authorising Officers must be "an assistant chief officer or investigations manager" or above.
- The Authorising Officers should not be directly involved in the investigation.

APPENDIX C i

Application Forms

Directed Surveillance

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary

Judicial Approval

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary

APPENDIX C ii

Application Forms

Covert Human Intelligence Sources (CHIS)

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary

~~APPENDIX C iii~~

~~Application Form for Communications Data~~

~~See Home Office website:~~

~~http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/communications-data1.doc?view=Binary~~

APPENDIX D

Codes of Practice and Government Guidance

All current Government Codes of Practice are available on the Gov.uk website:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

Protection of Freedom Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary

~~**Acquisition and Disclosure of**~~ **Communications Data** **Code of Practice**

See Home Office website:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

~~http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary~~

Appendix B

East Herts District Council

Regulation of Investigatory Powers Act 2000

Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Regulation of Investigatory Powers Act 2000 Policy
Author – name and title	James Ellis, Head of Legal & Democratic Services
Owner – name and title	James Ellis, Head of Legal & Democratic Services
Date	March 2023
Approvals	Executive
Version	2.0
Next Review Date	June 2024

East Herts Council

Regulation of Investigatory Powers Act 2000
Policy

Contents

1. Introduction

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ("RIPA") came into force on 25 September 2000 and sought to regulate covert investigation practices undertaken by a number of bodies, including local authorities.

This Policy is the framework on which East Herts Council ("the Council") applies the provisions of RIPA as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by the Investigatory Powers Commissioner's Office (the "IPCO") (formerly the Office of Surveillance Commissioners – OSC) and individual Services to deal with the specific issues of their service.

1.2 Background

The Human Rights Act 1998 requires the Council to have respect for the private and family life of citizens. However in rare cases, it may be lawful, necessary and proportionate for the Council to act covertly in ways that may interfere with an individual's rights.

The rights conferred by Article 8 of the Human Rights Act are not absolute rights, but qualified right, meaning that it is still possible for a public authority to interfere with those rights provided the following criteria are satisfied;

(a) It is done in accordance with the law
(b) It is necessary (as defined in this document); and
(c) It is proportionate (as defined in this document).

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

It is possible that unauthorised surveillance will be a breach of a person's right to privacy under Article 8. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not

obtained, the surveillance carried out will not have the protection that RIPA affords.

If the correct procedures are not followed;

- evidence may be disallowed by the courts,
- a complaint of maladministration could be made to the Ombudsman, and/or
- the Council could be ordered to pay compensation

It is therefore essential that this document, along with any further guidance that may be issued from time to time by the Head of Legal and Democratic Services, always be complied with.

1.3 Policy Review

RIPA and this document are essential for the effective, efficient and legal operation of the Council's covert surveillance activity. This document will, therefore be kept under annual review by the Head of Legal and Democratic Services.

Authorising Officers, as defined below, must bring any suggestions for the continuous improvement of this document to the attention of the Head of Legal and Democratic Services, at the earliest possible opportunity.

1.4 Scope

RIPA does not;

- Make unlawful anything that is otherwise lawful
- Impose any new statutory duties, or
- Prejudice or disapply any existing powers available to the Council to obtain information by any means not involving conduct that is governed by RIPA. (For example it does not affect the Council's current powers to obtain information from the DVLA or the Land Registry).

If RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, Employment Tribunal hearings and a complaint to either the Local Government Ombudsman or the

Investigatory Powers Tribunal. It therefore provides protection both for the Council and any officer who may have been involved in an investigation.

It should also be noted that the requirements of RIPA, and this policy, extends to external agencies working on behalf of the Council. Where such agencies are carrying out the Authority's statutory functions, the Authority remains liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so.

RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

- The use of Directed Surveillance
- The Use of Covert Human Intelligence Sources
- The Acquisition and Disclosure of Communications Data

2. Definition of Surveillance

"Surveillance" includes:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations or their other activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by, or with, the assistance of a surveillance device, which will include cameras, video, and listening or recording devices.

Surveillance can be either overt or covert.

2.1 Overt Surveillance

The overwhelming majority of surveillance undertaken by the Council will be done overtly, meaning there will be nothing secretive or hidden about the way it is conducted. In many cases officers will be going about Council business openly (e.g. a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if it continues.)

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 Head of Legal and Democratic Service or the Senior Responsible Officer

Use of body worn cameras should also be overt. Badges should be worn by officers stating body cameras are in use and it should be announced verbally that recording is taking place. In addition, cameras should only be switched on when recording is necessary e.g. when issuing parking tickets.

2.2 Covert Surveillance

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

3. Directed and Intrusive Surveillance

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
c) 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 RIPA to be sought for the carrying out of the surveillance.

3.2 Intrusive Surveillance

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

Surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or
b) where a device placed outside consistently provides information of the same or equivalent quality and detail as might be expected if it were in the premises or vehicle, or
c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device **OR** when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

A private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the council has no statutory powers to interfere with private property.

4. Identifying directed surveillance

You should ask yourself the following questions:

4.1 Is the surveillance overt or covert?

Refer to paragraphs 2.1 and 2.2 above. If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. If the proposed surveillance is covert in nature, then refer to paragraph 4.2 below.

4.2 Can the same outcome be achieved by overt means?

Does the surveillance have to be covert? If not, then you should proceed with overt surveillance, including the use of signs and other notification techniques so that the subject of the surveillance is aware it is taking place.

4.3 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.4 Is the surveillance likely to result in the obtaining of private information about a person?

Private information is defined in RIPA section 26 (10) as including any information relating to a person's private or family life.

The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8.

The Article also protects a right to identity and personal development and includes an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.5 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, an environmental crime officer would not require an authorisation to conceal themselves and observe a suspicious person which they came across in the course of a routine patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. Covert Human Intelligence Sources (CHIS)

A person is a covert human intelligence source ("CHIS") if;

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship if, and only if, the relationship is conducted in a

manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly if, and only if, it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

A member of the public who volunteers information to the Council is not a covert human intelligence source.

Likewise, members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS either as they are not usually required to establish or maintain a covert relationship.

It should be noted, however, that if the information provided is recorded as potentially useful or actionable, there is potential duty of care to the individual and the onus is on the public authority to manage human sources properly. Authorising Officers should be alive to the possibility of 'status drift'. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

5.1 Conduct and use

The conduct or use of CHIS must be authorised in accordance with RIPA.

Conduct of a CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information.

Use of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

The use of a juvenile CHIS may only be authorised for four months at a time[1].

[1] Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018/715

5.2 Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert 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).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, or an adult is observing a juvenile test purchase, this will require authorisation, as directed surveillance. In all cases, a prior risk assessment is essential in relation to any young person used for a test purchase.

5.3 Security and Welfare

Only the Chief Executive is able to authorise the use of vulnerable individuals and juvenile CHIS's. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the Covert Human Intelligence Source Code of Practice which can be found here.

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

5.4 Criminal Conduct Authorisations

The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 (CHIS(CC)A) received Royal Assent on 1 March 2021 and went live for the police on 15 September 2021. CHIS(CC)A amends the Regulation of

Investigatory Powers Act 2000 and provides an express power to authorise a CHIS to participate in conduct which would otherwise constitute a criminal offence. This power is known as a Criminal Conduct Authorisation (CCA). It is important to note that local authorities have not been given these powers and it is mentioned here for the avoidance of doubt.

6. Communications Data

Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer.

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this 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 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, the sending of a communication or breach of a person's privacy.

Further guidance can be found in paragraphs 3.3 to 3.13 of the Communications Data Code of Practice.

The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through National Anti-Fraud Network (NAFN) and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the Communications Data Code of Practice).

7. RIPA Authorisation Procedure

7.1 General

Directed surveillance and the use of CHIS must be lawfully carried out in strict accordance with the terms of the relevant authorisation and Magistrates Court approval.

The Council can only authorise directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:

a) S146 of the Licensing Act 2003 (sale of alcohol to children);
b) S147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
c) S147A of the Licensing Act 2003 (persistently selling alcohol to children); and
d) S7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under the age of 18)

The Council will only very rarely make use of CHIS so the applicant officer should consult the Head of Legal and Democratic Services before making

an application for a CHIS authorisation in order to ensure that the current statutory requirements and best practice are being observed.

Applications for authorisations and notices requesting communications data must be processed through the Council's Home Office accredited single point of contact ("SPoC"). As the need to obtain such information will only very occasionally arise the applicant officer should contact the Head of Legal and Democratic Services before making an application in order to ensure that current statutory requirements and best practice are being observed.

All applications for authorisation must be sought and granted before any surveillance activity takes place. The decision whether or not to authorise an application must not be taken with the benefit of hindsight. This should be borne in mind when submitting an application to the Magistrates' Court.

Once approved, the original authorisation and accompanying paperwork must be forwarded to the RIPA Co-Ordinator (Senior Solicitor – Corporate Legal Team) to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the central register.

7.2 Before Making the Application

Before making an application for an authorisation, the requesting officer must;

- read this policy document,
- determine whether the activity that they are proposing to conduct involves directed surveillance or the use of a CHIS,
- assess whether the activity will be in accordance with the law – is it governed by RIPA,
- assess whether the activity is necessary and why,
- assess whether the activity is proportionate.

If the activity can be conducted overtly or if a less intrusive option is available and practical, then that option should be pursued rather than obtaining a RIPA authorisation.

7.3 Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved.

Confidential information consists of personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Head of Legal and Democratic Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's spiritual welfare or matters of medical or journalistic confidentiality.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act 2000.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive or, in his absence, the person acting as the Head of Paid Service.

7.4 Who can give Authorisations?

Authorisations may only be given by the Authorising Officers listed in Appendix B. Only the Chief Executive can authorise the use of a CHIS, or the acquisition of confidential information (see paragraph 7.3 above).

Applications for the acquisition of Communications data can only be issued by a Home Office accredited single point of contact ("SPoC") (see paragraph 7.8 below)

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Head of Legal and Democratic Services before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training or a one-to-one meeting with the Head of Legal and Democratic Services, on such matters, will be kept by the Head of Legal and Democratic Services.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. Where an Authorising Officer authorises such an investigation or operation the central register will highlight this and the Commissioner or inspector will be notified of this during his or her next inspection

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of authorisations and associated documentation to the Head of Legal and Democratic Services, that these are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

7.5 Grounds for Authorisation

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant an authorisation for the carrying out of directed surveillance or for the use of a CHIS or for the obtaining or disclosing of communications data unless they have given **personal consideration** to the facts and believes:

a) that an authorisation is necessary, and
b) the authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Authorisation cannot be sought, and authority must not be given unless you are satisfied that the surveillance is "**proportionate**." You have to make sure that any interference with privacy is justified by the end being sought. Unless the benefit to be obtained from surveillance is significant, and unless the problem you are seeking to tackle is serious, the use of surveillance is unlikely to be proportionate.

The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and other minor offences will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the

authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities.

Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

7.6 Collateral Intrusion

Before authorising an investigation, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation; known as collateral intrusion. The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for an authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

7.7 Judicial Approval

The Council is only able to grant an authorisation or renewal to conduct covert surveillance. No authorisations, nor any surveillance granted under them, will take effect until judicial approval has been sought and granted by a Magistrates' Court.

Once the authorising officer has authorised the directed surveillance or CHIS, the investigating officer who completed the application form should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The investigating officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition the investigating officer will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the investigating officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate.

The Justice of the Peace will also consider whether there continues to be reasonable grounds.

The Justice of the Peace must also be satisfied that the person who granted the authorisation was an appropriate designated person and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for directed surveillance has been met.

The Justice of the Peace will record his/her decision on the order section of the judicial application/order form.
A copy of the RIPA form and judicial application/order form will be retained by the Court.

If the authorisation is approved the council may commence the activity.
If the Justice of the Peace refuses to approve the authorisation the council may not commence the activity although, if the reason for refusal is a technical error, the council may address this and reapply without going through the internal authorisation process again.

The Justice of the Peace may refuse to approve the authorisation, and quash it. The exercise of this power should not take place until the applicant has at least two business days from the date of the refusal to make representations.

7.8 Authorisation for Communication Data

The Act provides two different ways of authorising access to communications data; through an authorisation under Section 22(3) and by a provisional notice under Section 22(4).

An authorisation would, following judicial approval, allow the authority to collect or retrieve the data itself. A provisional notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An Authorising Officer decides whether or not an authorisation should be granted, or a provisional notice given.

An authorisation under Section 22(3) may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

Notices and, where appropriate, authorisations for communications data must be channelled through SPoC's. The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

The Council use the services of the National Anti-Fraud Network (NAFN) for all Communications Data enquiries and as such NAFN performs the role of a SPoC through their qualified SPoC officers. All applicants must be registered with NAFN via the NAFN website at www.nafn.gov.uk

Applications to obtain communications data should be made on the NAFN standard form available on the NAFN website and submitted in the first instance to the SPoC. If appropriate the SPoC will forward the application to a Council Authorising Officer for either the authorisation of conduct or the issuing of a notice.

If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will return the authorisation or notice to the SPoC who will then liaise with the applicant and the

postal/telecommunications company, after the appropriate Judicial Approval has been obtained. The disclosure of data under a notice will only be made to the Authorising Officer.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

8. Activities by other public authorities

The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9. Joint Investigations

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

a) wishes to use the Council's resources (e.g. CCTV), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources
b) wishes to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

10. Duration, reviews, renewals and cancellation of authorisations

10.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source
b) three months from the date of judicial approval for directed surveillance

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

10.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations.

Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

10.3 Renewals

If at any time before an authorisation ceases to have effect, it is necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 calendar months, beginning with the day when the original authorisation would

have expired. Magistrates Court approval is required before a renewal takes effect.

Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation and are approved by the Magistrates' Court. The renewal should be kept/recorded as part of the central record of authorisations.

The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

Authorisations can be renewed in writing shortly before the maximum period has expired. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

An authorisation cannot be renewed after it has expired.

A further requirement in relation to renewal of a CHIS is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source

For the purposes of making an Order, the Magistrates have considered the results of that review.

10.4 Cancellations

The Authorising Officer must cancel an authorisation if they become satisfied that the surveillance is no longer required or appropriate.

Authorisations should not be allowed simply to lapse. The duty to cancel a notice falls on the Authorising Officer who issued it.

The Authorising Officer must then cancel the Application without delay. When cancelling the authorisation the Authorising Officer is required to consider whether the surveillance was effective, necessary and met its

objectives. Cancellations must be made using the cancellation form and should briefly detail what product(s) resulted from the surveillance.

When cancelling an authorisation, the Authorising Officer must ascertain what recorded material has been obtained by the use of directed surveillance. The Authorising Officer should comment on the recorded material and how it is to be managed or used thereafter. If the matter is not proceeding to a prosecution, the Authorising Officer must be satisfied that any recorded material has been securely destroyed.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

11. Record Management

11.1 Central record of all Authorisations

The Head of Legal and Democratic Services shall hold and monitor a centrally retrievable record of all judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Head of Legal and Democratic Services to ensure that the records are regularly updated.

The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The Head of Legal and Democratic Services will monitor the submission of judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Head of Legal and Democratic Services, shall contain the following information:

a) the type of authorisation or notice
b) the date the authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;

e) the unique reference number (URN) of the investigation or operation;
f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) the date the authorisation or notice was cancelled.

11.2 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;
b) a record of the period over which the surveillance has taken place;
c) the frequency of reviews prescribed by the Authorising Officer;
d) a record of the result of each review of the authorisation or notice;
e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;
f) the date and time when any instruction was given by the Authorising Officer,
g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

11.3 Records relating to a CHIS

Proper records must be kept of the authorisation and use of a CHIS. An Authorising Officer must not agree an authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in

place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS.

The records shall contain the following information:

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant investigating authority other than the Council;
d) the means by which the source is referred to within each relevant investigating authority;
e) any other significant information connected with the security and welfare of the source;
f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g) the date when, and the circumstances in which, the source was recruited;
h) the identities of the persons who, in relation to the source;
    i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare
    ii. have a general oversight of the use made of the source (not to be the person identified in h) i.
    iii. have responsibility for maintaining a record of the use made of the source
i) the periods during which those persons have discharged those responsibilities;
j) the tasks given to the source and the demands made of him in relation to his activities as a source;
k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l) the information obtained by the conduct or use of the source;
m) any dissemination of information obtained in that way; and
n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Records which reveal the name(s) of the CHIS should only be disclosed to persons to the extent that there is a need for access to them; if legally necessary; or if ordered by any Court.

12. Retention and destruction

Generally, all material (in whatever media) produced or obtained during the course of investigations subject to RIPA authorisation should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000 and any other legal requirements, including those of confidentiality and the Council's policies and procedures regarding document retention.

Material obtained from properly authorised surveillance or a CHIS may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a CHIS or the obtaining or disclosure of communications data.

RIPA surveillance and CHIS records must be available for inspection by the Investigatory Powers Commissioner and retained for at least five years. Information obtained through covert surveillance or CHIS activity, and all copies, extracts and summaries which contain such material, should also be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out in section 9.5 of the Covert Surveillance and Property Interference Code of Practice.

If such information is retained, it should be reviewed at appropriate intervals in line with the relevant retention schedules to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material and the authorising officer, (in consultation with the SRO, is responsible for the retention / destruction decisions in connection with covertly acquired material.

13. Social Media Sites

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).

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 i.e. where privacy setting are available, but not applied, 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, 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..

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of any relevant guidance and the Council's separate policy regarding the use of **Social Networking Sites and Conduct of Investigations**.

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'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 engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

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.

As set out 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.'

14. Scrutiny of investigatory bodies

The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it.

The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at https://www.ipco.org.uk/

15. Elected Members

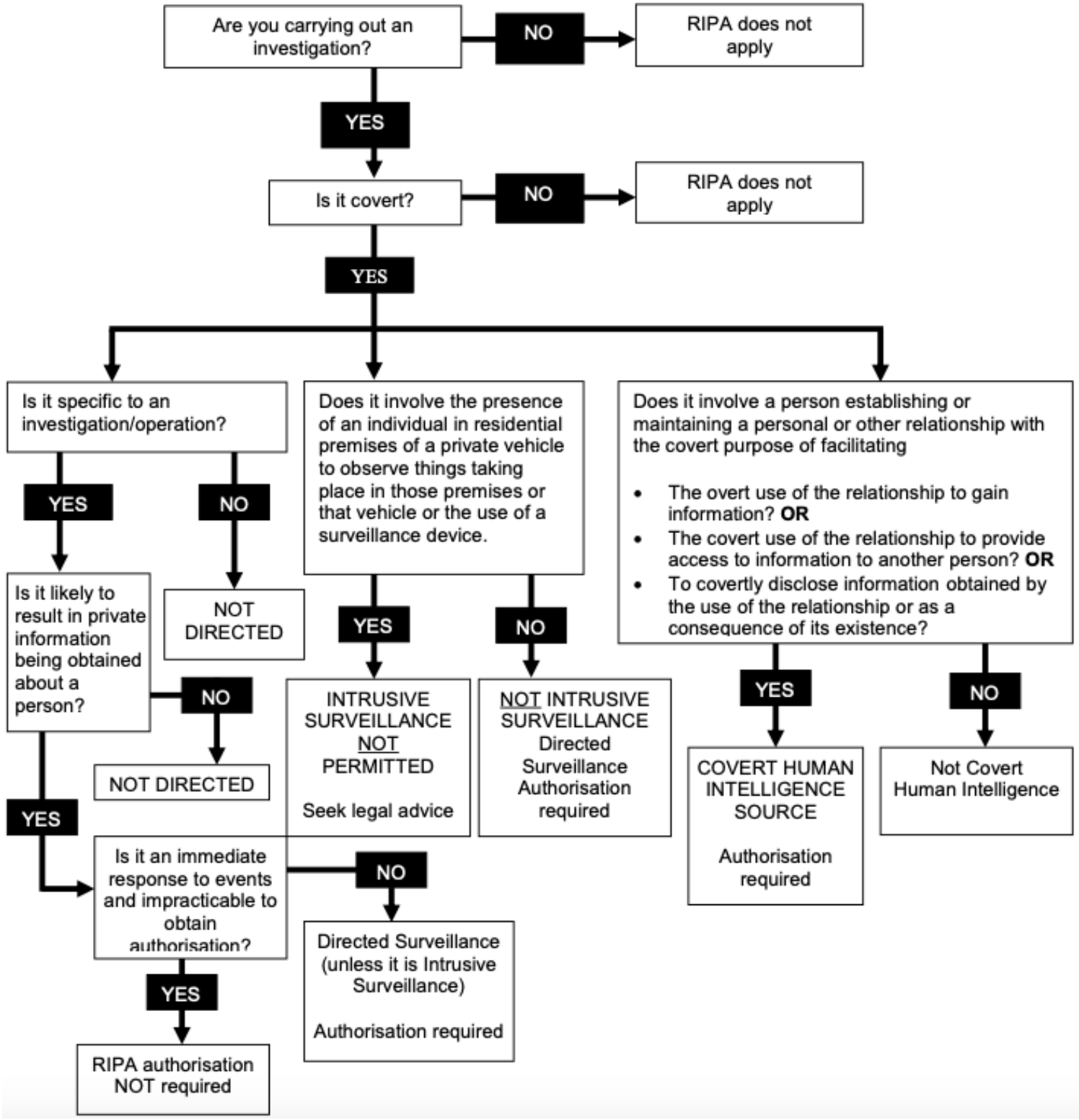
The elected members of the Council will review the council's use of RIPA and the authority's policy and guidance documents at least once a year. They will also be kept informed on a quarterly basis to ensure that it is being used consistently with the council's policy and that the policy remains fit for purpose. Members will not, however, be involved in making decisions on specific authorisations.

APPENDIX A

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000

Do you need Authorisation?



APPENDIX B

List of Authorised and Responsible Officers

RIPA Authorising Officers	Chief Executive, Deputy Chief Executive, Head of Operations, Head of Housing and Health Head of Planning
Authorising operations where confidential information may be obtained	Chief Executive only
CHIS Authorising Officer	Chief Executive only
CHIS Controller/Handler	Head of Operations Head of Housing and Health Head of Planning
Senior Responsible Officer	Head of Legal and Democratic Services

Please note:

- Where use of a CHIS is authorised, the head of the directorate carrying out the activity shall usually act as the CHIS Handler, with the CHIS Controller role being allocated by the Chief Executive.
- Authorising Officers must be "an assistant chief officer or investigations manager" or above.
- The Authorising Officers should not be directly involved in the investigation.

APPENDIX C i

Application Forms

Directed Surveillance

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary

Judicial Approval

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary

APPENDIX C ii

Application Forms

Covert Human Intelligence Sources (CHIS)

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary

APPENDIX D

Codes of Practice and Government Guidance

All current Government Codes of Practice are available on the Gov.uk website:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

Protection of Freedom Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary

Communications Data Code of Practice

See Home Office website:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

East Herts Council Report

Overview and Scrutiny Committee

Date of meeting: **Tuesday 21 March 2023**

Report by: **Scrutiny Officer**

Report title: **Overview and Scrutiny Committee - Draft Work Programme - 21 March 2023**

Ward(s) affected: **(All Wards);**

- **Summary** – This report considers actions for inclusion in the committee's existing Draft Work Programme and proposes amendments to the Draft Work Programme in supporting the Corporate Plan and "SEED" Priorities, approved by the Executive in February 2022.

RECOMMENDATIONS FOR OVERVIEW AND SCRUTINY COMMITTEE:

(A) The main agenda items for the next meeting be agreed.

(B) Members make additional recommendations for any items they wish to scrutinise; and

(C) The proposed Work Programme, as amended, at Appendix A be approved.

1.0 Proposal

1.1 **Appendix A** sets out the draft Work Programme which may be reviewed at any time.

1.2 The Corporate Plan was approved by Council in March 2022. A key function of the Overview and Scrutiny Committee is to hold the Executive to account for its decisions and to review existing policies and proposals for new policies. In deciding what items the committee should consider, Members should have regard to the Corporate and Forward Plans and what is due to be considered by the Executive.

2.0 Background

2.1 The draft agenda items for the remaining civic year are shown at **Appendix A.** Paragraph 5.21.2 of the Constitution sets out what the Overview and Scrutiny should take into account when setting its own programme. The timing of some items shown may have to change depending on the availability of data (e.g. from central government) external sources and Officers.

2.2 Members are welcome to submit a scrutiny proposal at any time by completing a Scrutiny Proposal Form (available from the Scrutiny Officer) which will provide Officers with sufficient information to assess if it is appropriate for Scrutiny and to ensure that their specific questions are addressed. The Scrutiny Officer will then liaise with Officers and the Overview and Scrutiny Committee Chairman to consider the best way to address the subject and complete a scoping document.

2.3 Members are also asked whether there is any training relevant to scrutiny or to the function and remit of the Overview and Scrutiny committee that they wish to suggest.

3.0 Reason(s)

3.1 This report provides an update on the current situation in relation to issues raised by Members.

4.0 Options

4.1 The Work Programme will be kept under review by the Committee throughout the coming year and is continually kept under review.

5.0 Risks

5.1 The establishment of an Overview an Scrutiny Committee is enshrined in the Local Government Act 2000 (section 9). The 2000 Act obliges local authorities to adopt political management systems with a separate Executive. Various sub sections of the 2000 Act set out the powers and duties for Overview and Scrutiny Committees including the right to investigate and make recommendations on anything which is the responsibility of the Executive. Legislative provisions can also be found in the Localism Act 2011 (Schedule 2) with options to retain or re-adopt a "committee system" (Section 9B).

5.2 Potential risks arise for the council if policies and strategies are developed and / or enacted without sufficient scrutiny. Approval of an updated work programme contributes to the mitigation of this risk by ensuring key activities of the council are scrutinised.

6.0 Implications/Consultations

6.1 Scrutiny is an important part of the local democratic process and represents the interests of residents. It holds the Executive to account on behalf of residents and helps review and improve the functions run by the Council and its local partners. With proper notification, Members of the public can up forward items for scrutiny (Section 5.19 of the Constitution) and if accepted by the Chairman are allowed to address Members for a maximum of 15 minutes.

6.2 The proposed Work Programme has implications for Members' time and the resources of the council devoted to scrutinising the issues included.

Community Safety
No

Data Protection
No

Equalities
Yes - Scrutiny of the services provided e.g. by registered providers of social housing will investigate how some of the most vulnerable people in the district, receive housing services.

Environmental Sustainability
Yes – the proposed Work Programme envisages the Overview Scrutiny Committee receiving reports on the progress of the council's environmental strategies.

Financial
No

Health and Safety
No

Human Resources
No

Human Rights
No

Legal
Yes – scrutiny is enshrined in statute (the Local Government Act 2000 as amended by the Localism act 2011)

Specific Wards
No

7.0 Background papers, appendices and other relevant material

7.1 **Appendix A** – Draft Work Programme

Contact Officer
James Ellis, Head of Legal and Democratic Services, Tel: 01279 502170. james.ellis@eastherts.gov.uk

Report Authors
Lorraine Blackburn and Katie Mogan, Scrutiny Officer, Democratic Services Manager. Tel: 01279 502172 and 07762 892098.
lorraine.blackburn@eastherts.gov.uk
katie.mogan@eastherts.gov.uk

"SEED" Priorities, Sustainability, Enabling, Encouraging and Digital by Default

Date	Report title/Strategy	SEED Priority	Background information	Officer invitee	Portfolio Holder	Executive Date
21 March 2023	Community Health and Wellbeing Plan 2023 – 2028	Sustainability	Update on the Plan	Head of Housing and Health	Councillor McAndrew (Executive Member for Environmental Sustainability	
21 March 2023	Air Quality Management Plan	Sustainability	Is the Air Quality management Plan being followed. Is it fit for purpose and is our website advertising the issue sufficiently for our residents? Are we fulfilling our statutory duty to deal appropriately with AQMA areas? - Question from Councillor C Wilson	Head of Housing and Health	Councillor McAndrew (Executive Member for Environmental Sustainability	
21 March 2023	RIPA	Sustainability	Update report	Head of Legal and Democratic Services	Councillor Cutting, (Executive Member for Corporate Services)	

Last updated 16 February 2023

"SEED" Priorities, Sustainability, Enabling, Encouraging and Digital by Default

21 March 2023	Information Governance and Data protection	Sustainability	Update report	Tyron Suddes, Information Governance and Data Protection Manager	Councillor Cutting, Executive Member for Corporate Services	
20 June 2023	Publish revised Parking Standards Supplementary Planning Document covering new development, including provision for e-v charging points at new residential properties and locations. (2a In the Corporate Plan).	Sustainability	Deferred at the request of the Head of Planning and Building Control – date for consideration by Members – to be confirmed. *The Head of Planning and Building Control has advised that "due to a lack of capacity in the planning policy team this work will now be undertaken by consultants. Officers are currently preparing a project brief. It is anticipated that work on the SPD will commence in March 2023"* ***Report to O&S Committee 20 June 2023 (email 3.2.23)***	Sara Saunders, Head of Planning and Building Control	Cllr Goodeve, Executive Member for Planning and Growth	8 November 2022

	We will ensure development is viable 3d. Delivery of the strategic sites allocated in the District Plan in accordance with the housing trajectory.	Encouraging Economic Growth	O&S on 8 November requested that this be deferred until after the May elections as to update new and returning Members? It might also be appropriate to have an update on the Transformation Programme and how this is progressing in the light of the savings to be achieved over the next few years??	Sara Saunders, Head of Planning and Building Control Steven Linnett, Head of Strategic Finance and Property	Cllr Kaye – Communities Cllr Goodeve – Planning and Growth	

"SEED" Priorities, Sustainability, Enabling, Encouraging and Digital by Default

7 November 2023	Pre- Planning Advice Process and Service	Sustainability	Updating the pre-app service was identified as an operational improvement when Planning underwent its recent service review. The restructure was completed at the end of August, and the Head of Service has been focussing their efforts on recruiting to vacant posts and resolving the backlog of planning applications. Report deferred from 8 November a with the consent of the Chairman. The Head of Planning and Building Control intends to provide a substantive report on this issue. Spring of 2023 has been provisionally suggested for this report . Update on new working practices Considered on 2 February 2021 – Chairman and VC posed the question "How are we going to improve the planning service considering the current increase in workload?" ***Full review incomplete. Head of Planning anticipates reporting November (email from HoS 6.2.23)***	Head of Planning and Building Control	Cllr Goodeve, Executive Member for Planning and Growth	

			Report to be presented to O&S to Committee 20 November 2023			

Members' views are sought regarding the timetabling of issues which Members may wish to review.

Wproc$/Stortford/BSWP/NPS/Overview and Scrutiny/2022-2023/Committee Work Programme Appendix