ISLINGTON

Resources Directorate
7 Newington Barrow Way, N7 7EP

Report of: Corporate Director Resources

Meeting of:	**Date:**	**Ward(s):**
Audit Committee	28 July 2020	N/A

Delete as appropriate		Non-exempt

THE APPENDICES TO THIS REPORT ARE EXEMPT AND NOT FOR PUBLICATION
The appendices to the report are not for publication because they contain exempt information under Schedule 12A of the Local Government Act (1972).

SUBJECT: IPCO Inspection Update

1. Synopsis

1.1 The Investigatory Powers Commissioners Office ("IPCO") has completed an inspection of the council's use of the Regulation of Investigatory Powers Act 2000 ("RIPA") and compliance with Home Office codes of practice.

1.2 The Investigatory Powers Commissioner ("IPC") has identified measures the council is required to take to safeguard data obtained under a covert surveillance authorisation.

2. Recommendation

2.1 To note the outcome of the IPCO's inspection of the council's surveillance activities and the necessary actions that the council is required to take within the suggested timelines as detailed in paragraph 5.8 of this report.

3. Background

3.1 RIPA provides a statutory framework regulating the use of covert surveillance by public authorities.

3.2 The Investigatory Powers Act 2016 ("IPA") governs the lawful obtaining of communications data by public authorities. Communications data is generated in the provision, delivery and maintenance of postal or telecommunications services but does not include the content of the communication.

3.3 The council can only undertake covert surveillance under RIPA if the proposed operation is authorised by one of the council's authorising officers and subsequently approved by a magistrate. The council's communications data requests must be authorised by the Office for Communications Data Authorisations.

3.4 The Investigatory Powers Commissioner ("the IPC") has responsibility for oversight of investigatory powers used under RIPA. The council was due to be inspected on 9 March 2020, but this physical inspection was cancelled. The inspection has instead been conducted remotely by telephone interview & desktop evaluation. Following completion of the inspection, the IPC issued a report on 5 June 2020. The IPC also issued a data assurance letter regarding data handling and retention safeguards relating to data obtained under RIPA and IPA.

4. The desktop inspection report

4.1 Unlike in previous inspections the IPC did not give the council specific actions or recommendations, but some recommendations and actions flow from the desktop inspection report.

4.2 **Recommendation 1** – to have a policy to govern 'non-RIPA' type investigations and operations.

RIPA does not apply to low level offences or to non-criminal investigations. The non-RIPA policy will cover covert surveillance related to such investigations and will follow a process similar to that set out under RIPA.

Action 1a – to draw up a 'non-RIPA' policy for sign off by the Senior Responsible Officer for inclusion in the council's RIPA policy & covert surveillance procedural notes.

Action 1b – when the 'non-RIPA' policy is signed off the RIPA Co-ordinating Officer to provide a briefing note for officers.

4.3 **Recommendation 2 –** ensure that officers engaged in investigatory or enforcement areas where RIPA considerations are not immediately apparent maintain their levels of knowledge and know whom to approach for guidance.

Action 2 - Senior Responsible Officer and RIPA Co-ordinating Officer to keep training requirements across the council under 6 monthly review.

5. The data assurance letter

5.1 In the desktop inspection letter, the IPC notes that the council has a number of policies and procedures in place to manage data gathered under RIPA and IPA and thus adheres to the safeguards outlined within the relevant codes of practice.

5.2 However, the IPC provided a separate letter that sets out additional areas they now expect to be followed and kept under regular review (see below). This report will address each area,

looking at how the council is currently complying and ensuring continued compliance and how we will ensure compliance where we are not fully compliant.

1) Review the safeguarding obligations in the relevant code of practice for any powers used by the council

2) Ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date

3) Ensure that the authorising officers for the council have a full understanding of any data pathways used for RIPA or IPA data

4) Ensure that all data obtained under IPA and RIPA is clearly labelled and stored on a data pathway with a known retention policy

5) Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the retention and disposal processes at the council

6) Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data

5.3 **Review the safeguarding obligations in the relevant code of practice for any powers used by the council**

This has been completed. In summary the three codes of practice set out the safeguards that should be applied in relation to the handling of material obtained through covert surveillance including the dissemination, copying, storage and destruction of private information.

The safeguards set out in each code have similarities and are closely aligned to the data protection principles: secure data storage and handling including ensuring that access is controlled on a 'need-to-know' basis; ensuring that only the information necessary is disclosed ('data minimisation'); ensuring that data is only copied when absolutely necessary; ensuring that data has retention periods applied to it and that data is securely destroyed when it is no longer required.

5.4 **Ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date**

The council has a number of policies and training that has been in place for a number of years that supports our compliance in this area.

- Records Management Policy

Sets out the rules governing how the council will store and manage its data. This is a general policy and does not set out how specific information will be stored.

- Information Asset Owners Policy

Sets out the expectations on Information Asset Owners (IAOs) (Service Directors and Heads of Service) with regards to managing the information they are responsible for. Specifically, that they own and effectively manage the risks to their information. This includes ensuring that access to data is controlled where required, that data is only used for its intended purpose and

that data is held in accordance with corporate standards. Information Asset Owners (IAO) are expected to attend IAO training every two years.

- Acceptable Use Policy (AUP)

Sets out the mandatory measures and requirements that are applicable to the use of the council's IT systems. The AUP sets out expectations on data storage which includes some detail as to where data should be stored and the use of removable media. All staff must read and accept the AUP before accessing their laptop for the first time. It is reissued to staff every 2 years or if there has been a significant update.

- Handling Special Category and Criminal Data Policy

Sets out how the council will ensure that special category and criminal conviction data will be protected. This policy is a requirement in the Data Protection Act 2018.

- Data Protection Policy

Sets out how the council complies with data protection legislation, including that data will be stored securely and ensuring that all staff understand their responsibilities.

- Keeping Information Secure Training

A mandatory eLearning course for all staff that includes guidance for staff in how to handle information securely.

- Corporate Retention Schedule

Sets out the retention period for council information. There are gaps in this document and it is currently under review.

Action 3a: The IG Team to review the policy and guidance for staff regarding sharing of data, obtained under a RIPA authorisation, with a specific focus on only providing the data that is necessary.

Action 3b: The retention schedule is updated so that RIPA and IPA is included and clearly defined.

5.4 **Ensure that the authorising officers for the council have a full understanding of any data pathways used for RIPA or IPA data**

Action 4: When the data mapping exercise described at 5.5 below is completed, authorising officers to be provided with a briefing.

5.5 **Ensure that all data obtained under IPA and RIPA is clearly labelled and stored on a data pathway with a known retention policy**

The Information Commissioner's Office recommends that organisations complete data mapping exercises to ensure that organisations can accurately identify how data flows through an organisation. This helps organisations know where their data is, who has access to it and how long it needs to be retained for.

Whilst processes around the control of RIPA authorisations and carrying out the investigation are very clear, the pathway and data flow has not been mapped. This means that the council can't be confident that data is not held in more than one location or that it's not held for longer than required. For example, a central record may be managed well and deleted once it's

reached its retention period, however a copy of the information may also reside in an email account.

Once a data flow is documented, it is easier to see where data resides and identify areas that are potentially not compliant. Clear retention can be identified and agreed and processes reviewed and communicated to relevant staff to ensure that expectations on management, storage and retention and deletion are clear.

Action 5a: Data mapping to be completed to ensure that the flow of data, resulting from a RIPA or IPA authorisation, is clear and identifies where data is stored.

Action 5b: Following the data mapping exercise identify where data should be stored and apply the agreed retention.

Action 5c: Audits are periodically undertaken to ensure that staff are complying with the agreed processes for managing RIPA and IPA data.

5.6 **Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the retention and disposal processes at the council**

Action 6: Briefing to be prepared for investigating officers and authorising officers regarding information to be included in RIPA and IPA authorisation requests regarding retention and disposal of the data obtained.

5.7 **Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data**

The council has not carried out a review of previous authorisations and therefore this is something that should be carried out. The data mapping and agreement on where the data should be stored and how long it should be retained will need to be completed before this step can be fully completed.

Action 7: Commence a full review of previous authorisations. Identify all locations that data is stored and (where retention has been exceeded) securely destroy the data. Data that is still within retention should be stored in the agreed location and have the agreed retention period applied.

5.8 In order to be compliant with the IPC recommendations the actions outlined in this report need to be implemented. A summary of these actions with timescales is set out below.

Number	Action	Owner	Timescale
Action 1a	To draw up a 'non-RIPA' policy for sign off by the Senior Responsible Officer for inclusion in the council's RIPA policy & covert surveillance procedural notes.	RIPA Co-ordinating Officer	31 August 2020

Action 1b	When the 'non-RIPA' policy is signed off the RIPA Co-ordinating Officer to provide a briefing note for officers.	RIPA Co-ordinating Officer	30 September 2020
Action 2	Senior Responsible Officer and RIPA Co-ordinating Officer to keep training requirements across the council under 6 monthly review.	RIPA Co-ordinating Officer	Every 6 months
Action 3a	The IG Team review the policy and guidance for staff regarding sharing of data, obtained under a RIPA authorisation, with a specific focus on only providing the data that is necessary.	Head of Information Governance and Data Protection Officer	31 July 2020
Action 3b	The retention schedule is updated so that RIPA and IPA is included and clearly defined.	Information Management Lead	31 August 2020
Action 4	When the data mapping exercise is completed, authorising officers to be provided with briefing.	RIPA Co-ordinating Officer	30 October 2020
Action 5a	Data mapping to be completed to ensure that the flow of data, resulting from a RIPA or IPA authorisation, is clear and identify where data is stored.	Head of Information Governance and Data Protection Officer	30 September 2020
Action 5b	Following the data mapping exercise identify where data should be stored and apply the agreed retention.	Information Management Lead (for coordination – each Investigating Manager to own 'their' data)	30 October 2020
Action 5c	Audits are periodically undertaken to ensure that staff are complying with the agreed processes for managing RIPA and IPA data.	Investigating Managers	Annually

Action 6	Briefing to be prepared for investigating officers and authorising officers regarding information to be included in RIPA and IPA authorisation requests regarding retention and disposal of the data obtained.	RIPA Co-ordinating Officer	30 October 2020
Action 7	Commence a full review of previous authorisations. Identify all locations that data is stored and (where retention has been exceeded) securely destroy the data. Data that is still within retention should be stored in the agreed location and have the agreed retention period applied.	Investigating Managers	1 January 2021

6. Implications

6.1 Financial implications:

There are no known financial implications.

6.2 Legal implications:

The IPCO inspection found that the council is complying with the legal requirements of RIPA and the Home Office codes of practice.

The data obtained under RIPA and IPA is subject to obligations under the Data Protection Act 2018.

6.3 Environmental implications and contribution to achieving a net zero carbon Islington by 2030:

There are no known environmental implications.

6.4 Resident Impact Assessment:

The council must, in the exercise of its functions, have due regard to the need to eliminate discrimination, harassment and victimisation, and to advance equality of opportunity, and foster good relations, between those who share a relevant protected characteristic and those

who do not share it (section 149 Equality Act 2010). The council has a duty to have due regard to the need to remove or minimise disadvantages, take steps to meet needs, in particular steps to take account of disabled persons' disabilities, and encourage people to participate in public life. The council must have due regard to the need to tackle prejudice and promote understanding.

A Resident Impact Assessment has not been completed because it is not relevant to this report.

7. Reason for recommendations

7.1 To comply with the recommendations flowing from the IPC inspection report and data assurance letter the council should implement the actions by the timelines outlined in paragraph 5.8.

Appendices: IPCO letters – 'Inspection of London Borough of Islington' and 'Assurance of data handling and retention safeguards'. (Exempt)

Final report clearance:

Signed by: 

Corporate Director Resources Date 9 July 2020

Report authors: Marina Lipscomb & Leila Ridley
Tel: 020 7527 32314/020 7527 8894
Email: marina.lipscomb@islington.gov.uk and leila.ridley@islington.gov.uk

Financial implications author: Steve Key
Tel: 020 7527 5636
Email: steve.key@islington.gov.uk

Legal implications author: Marina Lipscomb
Tel: 020 7527 3314
Email: marina.lipscomb@islington.gov.uk