Agenda Item No. 9

Audit Committee – 7 April 2014

Regulation of Investigatory Powers Act (RIPA) 2000

Summary of report:

This report is to:

- advise the Audit Committee of the outcome of the inspection of the Interception of Communications Commissioner's Office (IOCCO) which took place on 10 December 2013 and note the council's response; and

- provide the Audit Committee with a summary of surveillance activities undertaken by the council under the Regulation of Investigatory Powers Act (RIPA) 2000 for the 9 month period ending 31 December 2013.

Background papers:

Regulation of Investigatory Powers Act (RIPA) 2000 activity records.

Recommendations:

1. To note the outcome of the inspection of the Interception of Communications Commissioner's Office (IOCCO) which took place on 10 December 2013 and the council's response.

2. Note the council's use of the Regulation of Investigatory Powers Act (RIPA) 2000 and seek assurance from the Senior Responsible Officer that it is being used consistently with the council's policy and procedures.

Jamie Morris – Executive Director (Neighbourhood Services)
20 March 2014

Background

Where there is an interference by a local authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

The Home Office has strongly recommended that local authorities seek an authorisation where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation ensures that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Directed surveillance authorisations under Part II of the Regulation of Investigatory Powers Act (RIPA) 2000 may be granted in relation to covert surveillance undertaken in relation to a specific investigation or operation which is likely to result in the obtaining of private information about a person, and which is other than an immediate response to events or circumstances.

Regulation of Investigatory Powers Act (RIPA) 2000
Annual comparators 1 April 2010 – 31 March 2013 and 9 month period to 31 December 2013

The table at **Appendix 1** includes the general purpose or reason for which RIPA authority was granted and the number of authorities granted for each purpose or reason for the period. It is not possible to give further details as this may breach confidentiality legislation, interfere with the proper investigation of potential offenders or disclose other operational information which could hinder past, current or future activities, investigatory techniques or investigations.

In accordance with the council's policy and procedures on the Regulation of Investigatory Powers Act (RIPA) 2000, where surveillance pertaining to a non-criminal investigation into the conduct of an employee is required, officers are required to complete the appropriate forms and submit them for approval, but these are no longer considered to be RIPA authorisations. This follows advice given by the Office of Surveillance Commissioner in their inspection in March 2010. No such authorisations have been made in 2013/14 to date.

Interception of Communications Commissioner's Office

The council was subject to an IOCCO inspection on 10 December 2013. The inspection concluded that the council is acquiring communications data for a correct statutory purpose and for investigations where they have a clear duty and responsibility to conduct a criminal investigation. Overall the council has a satisfactory level of compliance with the act and code of practice, but there is room to improve the systems and procedures. The IOCCO report is detailed at **Appendix 2** and the council's response is detailed at **Appendix 3**.

Resource and legal considerations:

Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, S78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

Citizen impact:

Report scrutiny assists in demonstrating that the council and its officers are protected and provides an assurance to stakeholders about the security of the council's operations.

Performance and risk management issues:

Failure to implement these requirements may lead to adverse reports on future inspection and examination by the courts.

This report provides another layer of monitoring of the use of the Regulation of Investigatory Powers Act (RIPA) 2000 and therefore accountability of the officers is heightened.

Equality Implications:

None arising from this report.

Consultation:

This report is produced in accordance with the agreed work programme for the Audit Committee as detailed in the report 'The Roles and Responsibilities of the Audit Committee' which was agreed by Audit Committee on 24 June 2013.

Author:

Jamie Morris
Executive Director, Neighbourhood Services
☎ 01922 653203
✉ morrisjamie@walsall.gov.uk

Appendix 1

Regulation of Investigatory Powers Act (RIPA) 2000
Annual comparators 1 April 2010 – 31 March 2013 and 9 month period to 31 December 2013

	1 April 2010 – 31 March 2011 (Annual)	1 April 2011 – 31 March 2012 (Annual)	1 April 2012 - 31 March 2013 (Annual)	1 April 2013 – 31 December 2013 (9 months)
Housing benefit and / or council tax benefit investigation	16	16	4	0
Anti social behaviour enforcement	23	31	9	0
Trading standards – age restricted test purchasing (knives, cigarettes, alcohol, fireworks), taxis plying for hire, counterfeit goods, fly tipping, litter enforcement	15	19	18	7
Miscellaneous – staff working privately while absent on sick leave; insurance claims from injured parties	1	1	0	0
Total	55	67	31	7

Inspections under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

Name of Public Authority	Walsall Metropolitan Borough Council
Date of Inspection	10 December 2013
Inspectors	Richard Cloke and Ryan Tilly

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Anthony May. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objective of the inspection is to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

Statistics:

Number of applications which have been made during the previous 12 month period.	**2** **(15 in total since 2009)**
Number of Authorisations granted under each section of the Act during the previous 12 month period.	**0**
Number of Notices issued under each section of the Act during the previous 12 month period.	**S21 4(b) - 2** **S21 4(c) - 1**
Number of applications which have been rejected by a Designated Person during the previous 12 month period.	**0**

Staffing:

Senior Responsible Officer (SRO)	Jamie Morris, Executive Director Neighbourhoods
Accredited Officers (AOs) (indicate if full time AO, part time AO etc)	Lynda Purcell, Trading Standards Officer Steven Doyle, Trading Standards Officer (part time AOs)

Summary of Inspection Findings:

Walsall Metropolitan Borough Council has used its powers under Part I Chapter 2 of RIPA infrequently. The Inspectors were satisfied that the Council is acquiring communications data for a correct statutory purpose and for investigations where they have a clear statutory duty and responsibility to conduct a criminal investigation. Overall the Council has a satisfactory level of compliance with the Act and CoP, and consequently there is room to improve the systems and procedures.

The Inspectors examined all of the applications submitted since 2009. The applications were completed to an inconsistent standard overall. The majority were completed to a satisfactory standard. However a small minority were poorly completed and omitted some important details. In a number of cases the Inspectors requested and examined further background information in relation to the requests in order to satisfy themselves that they were necessary and proportionate. Recommendations have been made in the report to assist the Council to ensure that all applications are completed to the required standard in future.

The Accredited Officers (AOs) and the Designated Person (DP) had generally discharged their responsibilities effectively, ensuring that the Council acted in an informed and lawful manner when acquiring communications data. The one exception related to the giving of Notices by the DP. This requirement was misunderstood by the SPoC who were preparing the Notices after the applications had been approved by the DP. The Inspector advised that it is the statutory responsibility of the DP to issue the Notices and therefore it is important that they see them and endorse them in a clear and auditable way. Any Section 22(4) Notices which do not emanate from the DP constitute 'recordable' errors however it is important to outline that the Inspectors were satisfied that these errors had no bearing whatsoever on the justifications for acquiring the data.

The Inspectors were informed that the Council's Benefit Investigation Team is using the SPoC facility provided by the National Anti-Fraud Network (NAFN). IOCCO have made enquiries with NAFN and it does not appear that the Benefit Investigation Team has actually made any communications data requests under RIPA with NAFN to date, but they could well be making use of the other services that NAFN provide. The NAFN SPoC service has been funded by the Home Office who are encouraging all the local authorities to use the facility. Local Authorities can use the NAFN SPoC facility with confidence and in the full knowledge that the data will be obtained in accordance with the law. If the Council is already a member of NAFN, then the SPoC services provided by NAFN are open to all departments within the Council to use. It would be very unwise for the Council to have two separate regimes to acquire communications data and consequently a recommendation is made for the Chief Executive to review the communications data acquisition procedures across the whole Council. The Council should give serious consideration to solely using the NAFN SPoC facility.

The inspection findings are outlined in more detail in the following sections of the report. A number of recommendations arise from the inspection and they are mainly designed to

tighten or fine tune parts of the systems and processes and assist the public authority to achieve the best possible level of compliance with Part I Chapter II of RIPA and its associated CoP. The recommendations are shown in the last column of the inspection tables. Please note that recommendations are shaded red, amber or green. IOCCO have adopted this practice to enable public authorities to prioritise the areas where remedial action is necessary. The red areas are of immediate concern as they mainly involve serious breaches and / or non-compliance with the Act or CoP which could leave the public authority vulnerable to challenge. The amber areas represent non-compliance to a lesser extent. However remedial action must still be taken in these areas as they could potentially lead to breaches. The green areas represent good practice or areas where the efficiency and effectiveness of the process could be improved.

Summary of Recommendations: Red - 0; Amber - 5; Green - 1.

Areas Inspected:

1. Application Process

Acquisition of communications data under the Act involves four roles within a relevant public authority; the Applicant, the Designated Person (DP), the Single Point of Contact (SPoC) and the Senior Responsible Officer (SRO). The Act provides for two alternative means for acquiring communications data, by way of an Authorisation under Section 22(3) or a Notice under Section 22(4).

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Examination of Applications			
A number of applications will be randomly examined by the Inspection team to check that the correct process has been applied and that the data has been obtained lawfully, with the approval of a Designated Person (DP). Public authorities must restrict the use of their powers under Part I Chapter II to obtaining communications data for investigations where they have a clear statutory duty and responsibility to conduct a criminal investigation and they should never be used to investigate trivial offences.	**Yes**	**Applications examined:** All of the applications submitted since 2009 (15). The Inspectors were satisfied the communications data had been acquired for the correct statutory purpose i.e. Section 22(2)(b) 'for the prevention and detection of crime' and that the applications were submitted in relation to criminal offences which the public authority has a statutory duty to investigate. The Inspectors were satisfied that the correct process had been applied and that the data had been obtained lawfully, with the approval of a Designated Person (DP). The Inspectors concluded that the applications were completed to an inconsistent standard. The majority were completed to a satisfactory standard, but a small	

		minority were not completed to the required standard.	
Applicant			
The applicant should complete an application form, setting out for consideration by the designated person (DP), the necessity and proportionality of a specific requirement for acquiring communications data. (Para 3.3 CoP). Applications must include all of the requirements specified in Paragraphs 3.5 and 3.6 of the CoP. The Home Office and National Policing Data Communications Group (NPDCG) have produced a template application form.	**Yes**	**Application / System used:** The applications are completed electronically and forwarded to the SPoC. After completing the SPoC report the AOs print the applications for the DP who completes their considerations in writing. **The Inspectors advised that the Commissioner supports the use of email to manage the application process providing a clear audit trail exists. The SPoC can email the application and draft Notices to the DP who can then record his or her considerations and approval, insert the time and date of issue on any Section 22(4) Notices, and return the documents to the SPoC. It would be appropriate for the SPoC to centrally store the emails (and their attachments) from each stage of the application process electronically and only print a hard copy when it is required.**	**1**
Necessity: Applicants should outline a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together. A brief description of the investigation or operation may assist the DP to better understand the reason for the application. In a long term or complex investigation or operation it is important to set the application in context with the overall investigation or operation and set the scene and background. (See Home Office and NPDCG application guidance document).	**Partly**	There was a lack of background detail in a small number of the applications and as a result the link between the crime, suspect/s and communications addresses was often unclear. Applicants did not always specify the crime / offence under investigation (including the relevant legislation or Act) and this is a key part of the necessity test. The source of the communications address must also be outlined (i.e. how the communications address was identified). As a result of the omissions in some of the applications the Inspectors had to seek further clarification in relation to a number of the requests. On the basis of the further information received / examined, the Inspectors were satisfied that the requests were necessary. **Applicants must ensure that they follow the question sets and guidance prompts on the application form template to improve the overall standard of the application forms. The SPoC should provide a more robust guardian and gatekeeper role in**	**2**

		this respect to ensure the principle of necessity is sufficiently justified.	
Proportionality: Applicants should outline what is expected to be achieved from obtaining the data and how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. The specific date/time periods requested should be justified i.e. how these are proportionate. An explanation as to how the data will be used, once acquired, and how this will benefit the investigation will assist the justification. (See Home Office and NPDCG application guidance document).	**Partly**	On occasions the applicants inferred, but did not clearly outline their investigative objectives which is a key part of the proportionality test. Again, the Inspectors had to seek further clarification in relation to a number of the requests. On the basis of the further information received / examined, the Inspectors were satisfied that the requests were proportionate. **It is recommended that applicants should focus on what they are trying to achieve from obtaining the data in the proportionality section and should outline their objectives in clear and simple terms. The AO should provide appropriate advice to ensure the principle of proportionality is sufficiently justified.**	**3**
Collateral Intrusion: Applicants should consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstance. Applicants should be aware that that there will only ever be minimal collateral intrusion in relation to subscriber data or that none will be identified at the time the application is made. (See Home Office and NPDCG application guidance document).	**Partly**	Generally applicants have a good understanding that collateral intrusion is minimal in relation to subscriber data. However in the one application for service use data the applicant had not outlined how they intended to manage collateral intrusion. The Inspectors discussed this case in detail and were satisfied with how the data had been analysed and used. **Applicants should set out a clear succinct plan in relation to how they would manage the data by focusing on identifying the telephone numbers related to the objectives of the investigation.**	**4**
Were any examples provided in relation to how communications data has been used to good effect (i.e. what use has been made of the data acquired by the investigating officers? Did it lead to the identification of the offender? How was it of value to the investigation?)	**Yes**	Over a number of years there have been a wide range of investigations where communications data has been used to good effect. It has usually assisted to identify and locate suspects. For example in July 2012 an investigation into the disposal of waste contrary to the Environmental Protection Act 1990 (commonly referred to as fly tipping), identified that the waste originated from a local licensed premises. The investigator was having difficulty identifying the culprit due to the frequent turnover of licensee and managers. The current manager supplied a mobile telephone	

		number for the previous manager who he thought was named 'Mark'. Account information was acquired and identified Daniel Davies. A successful prosecution ensued at Walsall Magistrates Court on 02/09/13. Mr Davies was convicted of breaching his duty of care to ensure waste was appropriately disposed of and received a fine and costs totalling £2,243.	
Single Point of Contact (SPoC)			
The SPoC should promote efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. The SPoC should provide a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner. (Para 3.16 CoP).	**Partly**	The SPoC has ensured that the public authority acted in an lawful manner when acquiring communications data. However there is a need for the SPoC to provide a more robust guardian and gatekeeper function with regard to the quality of the applications. The data was acquired and disclosed in a timely fashion.	
The SPoC should provide objective judgement and advice to both the applicant and the DP. (Para 3.16 CoP). The SPoC should engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations. (Para 3.17 CoP).	**Yes**	Applicants are encouraged to speak to the SPoC prior to submitting applications.	
The SPoC should be in a position to fulfil the additional responsibilities outlined in Para 3.17 CoP. There should be a full audit trail of all actions taken by the SPoC.	**Yes**	The AOs have recently introduced SPoC logs and these are completed to a good standard. There is a good audit trail of the actions taken by the AOs from the start to the end of the process.	
The SPoC may be an individual who is also a DP. The SPoC may be an individual who is also an applicant. The same person should never be an applicant, a DP and a SPoC. Equally the same person should never be both the applicant and the DP. (Para 3.19 CoP).	**Yes**		
Designated Persons (DPs)			
A DP shall not grant an authorisation or give notice unless they believe that obtaining the data in question by the conduct authorised is proportionate to what is sought to be achieved by obtaining the data. (Section 22(5) Act). A DP must consider the application and record his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. (Para 3.7 CoP). The DP shall assess the necessity for any	**Yes**	**Approx no. of DPs:** 1 – To date all applications have been considered by John Beavon, Regulations Services Manager. If required the SRO would provide resilience. **Rank / Level of DPs:** Senior Service Manager. **In accordance with Statutory Instrument No. 480/2010:** Yes	

conduct to acquire or obtain data taking account of any advice provided by the SPoC. (Para 3.10 CoP).		The Inspectors were satisfied that the DP is discharging his statutory duties responsibly. The DP is completing his written considerations to a satisfactory standard.	
IOCCO recommends that DPs should tailor their written considerations to the individual applications to provide evidence that they have been given due consideration.	**Yes**	The DP is generally following the good practice guidance by tailoring his considerations to the individual applications. Occasionally the comments were generic in nature.	
DPs must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a DP of their office, rank or position in the relevant public authority may grant or give. (Para 3.9 CoP).	**Yes**		
DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations. (Para 3.11 CoP)	**Yes**	John Beavon is not involved in the investigations.	
Judicial Approval			
Section 37 of the Protection of Freedoms Act (POFA) (2012) specifies that where a relevant person has granted or renewed an authorisation under section 22(3), (3B) or (3F),or given or renewed a notice under section 22(4), the authorisation or notice is not to take effect until such time (if any) as the relevant judicial authority has made an order approving the grant or renewal of the authorisation or (as the case may be) the giving or renewal of the notice.	**Yes**	**Total Number of Applications processed since 1st November 2012:** 2 **Were all of the above applications subject to Judicial approval:** Yes **Did the relevant Judicial authority approve / refuse / quash the authorisations / notices:** All approved.	
The application to the relevant judicial approval must be made by the public authority that has granted the authorisation. The local authority will provide the relevant judicial authority with a copy of the original RIPA application, authorisation and/or notice. In addition, the local authority will provide the relevant judicial authority with a partially completed judicial application / order form (Annex B of Home Office guidance). The order	**Yes**	**Description of Process:** Papers including the judicial application, application, SPoC report, DPs considerations and notice/s are emailed to the Court Services requesting a hearing. Usually within 5 working days an AO and the applicant meet with a District Judge in Chambers to consider the application.	

section of this form will be completed by the judicial authority and will be the official record of the decision.			
The original RIPA application, authorisation and / or notice must be retained by the local authority so that it is available for inspection by IOCCO and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The local authority will need to retain a copy of the judicial application / order form after it has been signed by the relevant judicial authority. The local authority may choose to serve the judicial order form on the CSP, along with the relevant authorisation or notice, to enable the CSP to be assured that judicial approval has been obtained. If the magistrate has included sensitive details about the investigation on the judicial order form, the SPoC may elect to just provide the CSP with the details of the judicial approval (i.e. date / time approval, name of magistrate / court etc).	**Yes**		
Content of Section 22(3) Authorisations and Section 22(4) Notices			
An authorisation must comply with all of the requirements outlined in Section 23(1) of the Act and Paragraphs 3.28, 3.43 & 3.44 of the CoP.	**N/A**	This method of conduct has not been used by the Council.	
A notice must comply with all of the requirements outlined in Section 23(2) of the Act and Paragraphs 3.37, 3.43 & 3.44 of the CoP.	**Yes**	Home Office and NP DCG template is in use.	
The 'giving of a notice' means at the point at which a DP determines that a notice should be given to a CSP (Para 3.35 CoP). A notice should emanate from the DP and be endorsed in a clear and auditable manner.	**No**	This requirement was misunderstood by the SPoC. The AOs were preparing the Notices after the applications had been approved by the DPs. The Inspector advised that it is the statutory responsibility of the DP to issue the Notices and therefore it is important that they see them and endorse them in a clear and auditable way. Any Section 22(4) Notices which do not emanate from the DP constitute 'recordable' errors. It is important to outline that these errors had no bearing on the actual justifications for acquiring the data which had been approved by the DP. Nevertheless the Council will always want to ensure that they act fully in accordance with the law. **The SPoC must ensure that in future all Notices are drafted and sent to the DP with the applications**	**5**

		in order for them to be formally issued by the DP. Any Section 22(4) Notices which did not emanate from the DPs constitute 'recordable' errors and these should be duly recorded by the SPoC.	
SPoCs should be mindful when drafting authorisations and notices to ensure the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful. A notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do. (Section 22(7) Act, Para's 3.29 & 3.38 CoP)	**Yes**		
Duration, Renewal & Cancellation of Section 22(3) Authorisations and Section 22(4) Notices			
Relevant to all authorisations and notices is the date upon which authorisation is granted or notice given. From that date, when the authorisation or notice becomes valid, it has a validity of a maximum of one month (see footnote 57 CoP). This means the conduct authorised should have been commenced or the notice served within that month. (Para 3.42 CoP).	**Yes**		
Any valid authorisation or notice may be renewed at any time before the end of the period of one month applying to that authorisation or notice, for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing. (Sections 23(5), 23(6) & 23(7) Act, Para 3.46 CoP).	**N/A**	This process has not been used to date.	
Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future, The reasoning for seeking renewal should be set out in an addendum to the application. Where a DP is granting a further authorisation or giving a further notice they should have considered why it is necessary and proportionate to continue with the acquisition of the data and record the date, and when appropriate, the time of the renewal. (Para 3.47 & 3.48 CoP).	**N/A**		
Where a DP is satisfied that it is no longer necessary or proportionate to acquire the communications data he shall cancel the notice or withdraw the authorisation. (Section 23(8) Act, Para's	**Yes**		

3.49, 3.50, 3.52 & 3.53 CoP). Reporting of a cancellation to a CSP may be undertaken on a DPs behalf by the SPoC, but in such cases the DP must confirm the decision in writing or in a manner that produces a record of the notice or authorisation having been cancelled or withdrawn by the DP.			
A cancellation notice must include the details outlined in Paragraph 3.51 of the CoP. A withdrawal of an authorisation must include the details outlined in Paragraph 3.54 of the CoP.	**N/A**		
National Priority Grading System (NPGS)			
Where relevant, the Data Communications Group (DCG) NPGS should be applied to requests for communications data correctly and fairly. (See Footnote 40 of the CoP). The emphasis within Grade 1 and Grade 2 is that the urgent provision of the specific communications data will have an immediate and positive impact on the investigation.	**Yes**	All applications submitted as Grade 3.	
Streamlining Procedures			
The streamlining procedure outlined in Paragraph 3.30 of the CoP should be used to reduce unnecessary bureaucracy and speed up the collection of the data when acquiring subscriber data under Section 21(4)(c). This procedure assists with number porting issues and enables the AOs to be more proactive when acquiring subscriber information by widening the data capture. In these instances it may be pertinent to acquire the data in stages. Furthermore, it is often good practice to check with the applicant before the data capture is widened because the direction of the investigation may have changed since the application was submitted or the user of the phone or communications address may have been identified through some other means.	**N/A**	This procedure has not been used by the Council to date. It would not be beneficial for the Council to use the streamlining procedures due to the low volume of requests.	
The streamlining procedure outlined in Paragraphs 3.31 and 3.32 of the CoP which enable a DP to pre-authorise future subscriber checks at the same time as he or she is approving an application for service use or traffic data under Sections 21(4)(a) or (b) of RIPA, should be used to reduce unnecessary bureaucracy and speed up the collection of the data.	**N/A**	This procedure has not been used by the Council to date. It would not be beneficial for the Council to use this streamlining procedure due to the low volume of service use requests.	
The applicant must outline why it is necessary and proportionate to either	**N/A**		

widen the data capture under Section 21(4)(c), or obtain the consequential 'future' subscribers in their application. In the latter case they should outline what analytical work they intend to conduct on the service use / traffic data to identify the relevant numbers. It is important that the SPoC gives appropriate advice to the DP and that the DP fully understands what he or she is approving in the application form.			
The AOs should spot check the schedules to assure the integrity of the process, i.e. to check that the communications addresses derive from the original service use / traffic data requests and that secure open source checks have been conducted. This should provide a good safety net. Furthermore if an AO finds evidence that applicants or analysts are not following the correct procedures then this should be brought to the attention of the SRO.	**N/A**		

2. Training

It is important for all persons involved in the process to receive training and guidance to ensure that communications data is acquired lawfully in accordance with the Act and CoP and used effectively in support of investigations.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
The SPoC is either an accredited officer (AO) or group of AOs trained to facilitate lawful acquisition of communications data. All AOs must complete a course of training and have been issued a SPoC PIN number. (Para 3.15 CoP). When an AO leaves the SPoC their PIN number should be removed from the list of approved AOs.	**Yes**	**PIN list checked:** Yes – Both AOs on the approved list.	
DPs must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II of Part I RIPA and its associated CoP. (Para 3.8 CoP).	**Yes**		
SPoCs should make efforts to ensure applicants are appropriately trained in the acquisition of communications data.	**Yes**	Applicants are encouraged to contact the SPoC before submitting applications and have access to the Home Office DCG guidance document for applicants and DPs. There is more work to be done to ensure that applicants meet the requirements	

		when submitting applications.	

3. Keeping of Records

There are clear rules which must be followed in relation to the keeping of records and these procedures include the recording and reporting of errors. See Chapter 6 of the CoP for further information.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Records to be kept			
Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date, and where appropriate the time, when each notice or authorisation is given or granted, renewed or cancelled. (Para 6.1 CoP).	**Yes**		
Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner. There records must be available for inspection by the Commissioner (Para's 6.1 & 6.2 CoP).	**Yes**		
Errors			
Where communications data is acquired or disclosed wrongly a report must be made to the Senior Responsible Officer (SRO) and then to the Commissioner ("reportable error") using the Error Reporting Form within no more than five working days of the error being discovered. (Para's 6.13 & 6.17 CoP). The error report must contain all of the details outlined in Para 6.18 of the CoP.	**Yes**	**No. errors 'reported' in previous 6 months:** 0 The Inspectors discussed the difference between recordable and reportable errors and provided the Council with the reportable errors template.	
In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ("recordable error"). These records must be available for inspection by the Commissioner (Para 6.14 CoP). The records must include the details outlined in Para 6.20 of the CoP.	**Yes**	**No. errors 'recorded' in previous 6 months:** 0 **Nature of errors (i.e. applicant, SPoC, CSP etc):** As outlined earlier in the report, none of the Section 22(4) Notices emanated from the DP and these instances constitute 'recordable' errors. The SPoC is now aware of this requirement and will now ensure the correct process is applied.	
Where material is disclosed by a CSP in	**N/A**	The Inspectors provided suitable	

error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, the material and any copy of it should be destroyed as soon as the report to the Commissioner has been made. (Para 6.21 CoP).		advice concerning this baseline for future reference.	
Excess Data			
Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority. If having reviewed the excess data it is intended to make use of it in the course of the investigation an applicant must set out the reason(s) for needing to use that material in an addendum to the original application. The DP will then consider the reason(s) and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. (Para's 6.23 to 6.25 CoP).	**N/A**	The Inspectors provided suitable advice concerning this baseline for future reference.	

National Anti-Fraud Network (NAFN) Single Point of Contact (SPoC)

During the inspection the Inspector discussed the SPoC facility which NAFN provides. NAFN has received funding from the Home Office so that it can act for any local authority which wishes to use its services and its AOs have been specially trained to the same standard as their police counterparts. NAFN uses an electronic system (Focus) to manage the applications and this system is used by a number of police forces and is fit for purpose. The NAFN AOs are also able to access a number of the online systems provided by the CSPs and therefore the data can be retrieved very quickly and with less expense. NAFN is inspected on an annual basis by IOCCO and has a very good level of compliance with the Act and CoP. They are providing a good service to their local authority members who can use the NAFN SPoC facility with confidence and in the full knowledge that the data will be obtained in accordance with the law. The Home Office is encouraging all local authorities to use the facility. All of the records can be accessed and examined by the IOCCO inspectors from the NAFN offices. The Senior Responsible Officer (SRO) at NAFN is responsible for the integrity of the SPoC system and processes. However the Interception of Communications Commissioner believes that it is important for each local authority that uses NAFN to still appoint a Senior Responsible Officer (SRO) to oversee the process. If any issues arise from the inspection of the NAFN SPoC in relation to an individual local authority, the Inspectors will engage with that local authority's SRO to resolve them. The NAFN SPoC should inform the local authorities who are using their facility when an inspection is due to take place and should of course disseminate the findings.

The Inspectors were informed that the Council's Benefit Investigation Team is already using the SPoC facility provided by the National Anti-Fraud Network (NAFN). IOCCO have made enquiries with NAFN and it does not appear that the Benefit Investigation Team has actually made any communications data requests under RIPA with NAFN to date, but they could well be making use of other services that NAFN provide. If the Council is already a member of NAFN, then the SPoC services provided by NAFN are open to all departments

within the Council to use. **It would be very unwise for the Council to have two separate regimes to acquire communications data and consequently it is recommended that the Chief Executive should review the communications data acquisition procedures across the whole Council with a view to giving serious consideration to solely using the NAFN SPoC facility (Recommendation 6).**

IOCCO will await notification of any decision concerning the use of the NAFN SPoC facility in order to facilitate future inspection planning and the collection of annual statistics on behalf of the Commissioner.

Freedom of Information Act (FOIA)

IOCCO is not a "public authority" for the purpose of the FOIA. It is therefore outside the reach of the Act, but it is appreciated that public authorities are not and that they may receive requests for disclosure of our reports. In the first instance the SRO should follow the procedure which is outlined in Paragraph 8.5 of the CoP (Part I Chapter II of RIPA). No disclosure should take place until IOCCO have been fully consulted as it is very important that requests under the FOIA are dealt with in a consistent manner.

Conclusion & Requirement for Action:

IOCCO are extremely grateful for the excellent assistance and cooperation received during this inspection. The recommendations from this inspection are appended to the report in a schedule. It would be appreciated if you would ensure that the Senior Responsible Officer (SRO) oversees the implementation of the recommendations and ensures the schedule is completed and returned electronically to ch2.inspectorate@iocco.gsi.gov.uk by 9th April 2014. In light of the satisfactory level of compliance it will not be necessary to conduct a further inspection for at least 18 months. If the Council decides to use the NAFN SPoC Service to manage its requirements in future no inspection will be necessary.

Appendix 3

Walsall Council

Neighbourhood Services

Our Ref: JM/LS
Date:
Ask for: Jamie Morris
Direct Line: (01922) 653203

DRAFT

Mr. Ian Mills
IOCCO Secretariat
Interception of Communication Commissioners Office

Dear Mr. Mills,

Inspection Report 10th December 2013

Thank you for your report received on the 11 February 2014 regarding the inspection of Walsall Council carried out by Richard Cloke and Ryan Tilly.

The report makes six recommendations which are attached to this letter together with our intended course of action.

The inspection report will be reported to the next available meeting of the Council's Audit Committee who will require me to update them on the progress in implementing these recommendations.

We are grateful for the advice and recommendations received from Mr. Coke and Mr. Tilly on how we can ensure continued good practice in our use of communication data.

Yours sincerely

Jamie Morris
Executive Director

The Civic Centre, Darwall Street, Walsall WS1 1TP
Tel: (01922) 653203 Fax: (01922) 615737

Recommendations for Walsall Metropolitan Borough Council as a result of the inspection conducted on 10th December 2013

No	Recommendation	Achieved (Yes / No / Partly)	Description / Comments
1.	Page 4 The Inspectors advised that the Commissioner supports the use of email to manage the application process providing a clear audit trail exists. The SPoC can email the application and draft Notices to the DP who can then record his or her considerations and approval, insert the time and date of issue on any Section 22(4) Notices, and return the documents to the SPoC. It would be appropriate for the SPoC to centrally store the emails (and their attachments) from each stage of the application process electronically and only print a hard copy when it is required.	Yes	We agree with this recommendation. We have produced a flow chart of the new electronic procedure to be implemented with immediate effect. The SPoC will store the e mails (and their attachments) from each stage of the application process electronically in a central and secure folder. In place 07/03/2014
2.	Page 4 Applicants must ensure that they follow the question sets and guidance prompts on the application form template to improve the overall standard of the application forms. The SPoC should provide a more robust guardian and gatekeeper role in this respect to ensure the principle of necessity is sufficiently justified.	Yes	Guidance will be issued to all applicants to ensure that future applications contain all relevant background details. The SPoCs will also check that this is carried out. In place 07/03/2014

3.	Page 5 It is recommended that applicants should focus on what they are trying to achieve from obtaining the data in the proportionality section and should outline their objectives in clear and simple terms. The AO should provide appropriate advice to ensure the principle of proportionality is sufficiently justified.	Yes	Guidance will be issued to all applicants to ensure that future applications contain all relevant background details. The SPoCs will also check that this is carried out. In place 07/03/2014
4.	Page 5 Applicants should set out a clear succinct plan in relation to how they would manage the data by focusing on identifying the telephone numbers related to the objectives of the investigation.	Yes	Guidance will be issued to all applicants to ensure that they understand how to manage collateral intrusion. The SPoCs will also check that this is carried out. In place 07/03/2014
5.	Page 8 The SPoC must ensure that in future all Notices are drafted and sent to the DP with the applications in order for them to be formally issued by the DP. Any Section 22(4) Notices which did not emanate from the DPs constitute 'recordable' errors and these should be duly recorded by the SPoC.	Yes	All notices will be sent to the designated person to be formally issued. All future applications from 10/12/2013
6.	Page 13 It would be very unwise for the Council to have two separate regimes to acquire communications data and consequently it is recommended that the Chief Executive should review the communications data acquisition procedures across the whole Council with a view to giving serious consideration to solely using the NAFN SPoC facility.	No	This has now been reported to the corporate management team on 20 March 2014. The council has decided to use NAFN as its sole source for communications data