DEVON & SOMERSET
FIRE & RESCUE AUTHORITY

M. Pearson
CLERK TO THE AUTHORITY

To: **The Chair and Members of the Audit & Performance Review Committee**

(see below)

SERVICE HEADQUARTERS
THE KNOWLE
CLYST ST GEORGE
EXETER
DEVON
EX3 0NW

Your ref :
Our ref : DSFRA/MP/SY
Website : www.dsfire.gov.uk

Date : 28 February 2020
Please ask for : Sam Sharman
Email : ssharman@dsfire.gov.uk

Telephone : 01392 872200
Fax : 01392 872300
Direct Telephone : 01392 872393

AUDIT & PERFORMANCE REVIEW COMMITTEE
(Devon & Somerset Fire & Rescue Authority)

Wednesday, 4 March, 2020

A meeting of the Audit & Performance Review Committee will be held on the above date, **commencing at 10.00 am in Committee Room B, Somerset House, Service Headquarters, Exeter** to consider the following matters.

M. Pearson
Clerk to the Authority

SUPPLEMENTARY AGENDA No. 1

PLEASE REFER TO THE NOTES AT THE END OF THE AGENDA LISTING SHEETS

13 **Authority Policy for the Regulation of Investigatory Powers Act 2000 (RIPA) - Further Considerations (Acquisition of Communications Data under the Investigatory Powers Act [IPA] 2016) (Pages 1 - 6)**

Report of the Director of Governance & Digital Services (APRC/20/7(a)) attached. This report should be considered in conjunction with report APRC/20/7 (Authority Policy for Regulation of Investigatory Powers Act 2000 [RIPA] – Review).

MEMBERS ARE REQUESTED TO SIGN THE ATTENDANCE REGISTER

Membership:-

Councillors Healey MBE (Chair), Clayton, Napper, Prowse (Vice-Chair), Saywell, Way and Wheeler.

NOTES	
1.	**Access to Information** Any person wishing to inspect any minutes, reports or lists of background papers relating to any item on this agenda should contact the person listed in the "Please ask for" section at the top of this agenda.
2.	**Reporting of Meetings** Any person attending a meeting may report (film, photograph or make an audio recording) on any part of the meeting which is open to the public – unless there is good reason not to do so, as directed by the Chair - and use any communication method, including the internet and social media (Facebook, Twitter etc.), to publish, post or otherwise share the report. The Authority accepts no liability for the content or accuracy of any such report, which should not be construed as representing the official, Authority record of the meeting. Similarly, any views expressed in such reports should not be interpreted as representing the views of the Authority. Flash photography is not permitted and any filming must be done as unobtrusively as possible from a single fixed position without the use of any additional lighting; focusing only on those actively participating in the meeting and having regard also to the wishes of any member of the public present who may not wish to be filmed. As a matter of courtesy, anyone wishing to film proceedings is asked to advise the Chair or the Democratic Services Officer in attendance so that all those present may be made aware that is happening.
3.	**Declarations of Interests at meetings (Authority Members only)** If you are present at a meeting and you are aware that you have either a disclosable pecuniary interest, personal interest or non-registerable interest in any matter being considered or to be considered at the meeting then, unless you have a current and relevant dispensation in relation to the matter, you must: (i) disclose at that meeting, by no later than commencement of consideration of the item in which you have the interest or, if later, the time at which the interest becomes apparent to you, the existence of and – for anything other than a "sensitive" interest – the nature of that interest; and then (ii) withdraw from the room or chamber during consideration of the item in which you have the relevant interest. If the interest is sensitive (as agreed with the Monitoring Officer), you need not disclose the nature of the interest but merely that you have an interest of a sensitive nature. You must still follow (i) and (ii) above. Where a dispensation has been granted to you either by the Authority or its Monitoring Officer in relation to any relevant interest, then you must act in accordance with any terms and conditions associated with that dispensation. Where you declare at a meeting a disclosable pecuniary or personal interest that you have not previously included in your Register of Interests then you must, within 28 days of the date of the meeting at which the declaration was made, ensure that your Register is updated to include details of the interest so declared.
4.	**Part 2 Reports** Members are reminded that any Part 2 reports as circulated with the agenda for this meeting contain exempt information and should therefore be treated accordingly. They should not be disclosed or passed on to any other person(s). Members are also reminded of the need to dispose of such reports carefully and are therefore invited to return them to the Committee Secretary at the conclusion of the meeting for disposal.
5.	**Substitute Members (Committee Meetings only)** Members are reminded that, in accordance with Standing Order 37, the Clerk (or his representative) must be advised of any substitution prior to the start of the meeting. Members are also reminded that substitutions are not permitted for full Authority meetings.

REPORT REFERENCE NO.	**APRC/20/7(a)**
MEETING	**AUDIT & PERFORMANCE REVIEW COMMITTEE**
DATE OF MEETING	**4 MARCH 2020**
SUBJECT OF REPORT	**AUTHORITY POLICY FOR REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) – FURTHER CONSIDERATIONS (ACQUISITION OF COMMUNICATIONS DATA UNDER THE INVESTIGATORY POWERS ACT [IPA] 2016)**
LEAD OFFICER	**Director of Governance & Digital Services**
RECOMMENDATIONS	***(a). That the amendment (appended to this report) required to align the Authority's policies and procedures for the acquisition of communications data with those now in place under the Investigatory Powers Act 2016 be approved;*** ***(b). that the Clerk be authorised to make other consequential amendments (to refer, where necessary, to the Investigatory Powers Act 2016) to the Authority's policies and procedures.***
EXECUTIVE SUMMARY	Subsequent to publication of the agenda for this meeting, confirmation has been received that the revised procedure for the acquisition of communications data, as introduced by the Investigatory Powers Act 2016, is now in force. The revised procedure retains the three key roles of Applicant, Senior Point of Contact (SPoC) and Authorising Individual as per the previous RIPA regime but introduces a new authorisation process (by the Office for Communications Data Authorisations) for the acquisition of communications data in non-urgent circumstances. Appended to this report is the relevant section of the Authority's policy, amended to reflect the new procedures and based on the relevant Home Office Code of Practice. Other consequential amendments to the policy (specifically, to refer, where necessary, to the Investigatory Powers Act 2016) will also be required.
RESOURCE IMPLICATIONS	There is a requirement to ensure that relevant officers receive appropriate training and that sufficient awareness-raising is undertaken to promote understanding of the processes to be followed to obtain RIPA and IPA authorisations. Any costs associated with the above will be met from within existing resources.
EQUALITY RISKS AND BENEFITS ANALYSIS (ERBA)	The contents of this report are considered compatible with existing equalities and human rights legislation.
APPENDICES	A. Authority Policy RIPA and IPA Policy – Revised Section on process for the acquisition of communications data under the Investigatory Powers Act [IPA] 2016. (***NOTE***: a copy of the full Authority RIPA and IPA policy can be a made available on request).

LIST OF BACKGROUND PAPERS	A. Regulation of Investigatory Powers Act 2000. B. Investigatory Powers Act 2016. C. Home Office Communications Data Code of Practice (November 2018). D. Report DSFRA/14/21 (Regulation of Investigatory Powers Act [RIPA] 2000 – Revised Authority Policy) to the full Authority meeting held on 17 December 2014 (and the Minutes of that meeting). E. Report APRC/15/1 (Regulation of Investigatory Powers Act [RIPA] 2000 - Revised Authority Policy) to the Audit & Performance Review Committee meeting held on 6 February 2015 (and the Minutes of that meeting). F. Report APRC/17/18 (Authority Policy for Regulation of Investigatory Powers Act 2000 [RIPA]) to the Audit & Performance Review Committee meeting held on 12 September 2017 (and the Minutes of that meeting). G. Report APRC/18/9 (Authority Policy for Regulation of Investigatory Powers Act 2000 [RIPA] – outcome of recent inspection) to the Audit & Performance Review Committee meeting held on 26 April 2018 (and the Minutes of that meeting). H. Report APRC/19/9 (Authority Policy for Regulation of Investigatory Powers Act 2000 [RIPA] – Review) to the Audit & Performance Review Committee meeting held on 10 May 2019 (and the Minutes of that meeting). I. Report APRC/20/7 (Authority Policy for Regulation of Investigatory Powers Act 2000 (RIPA) – Review) to this meeting of the Committee.

MIKE PEARSON
Director of Governance & Digital Services

ACQUISITION OF COMMUNICATIONS DATA UNDER THE INVESTIGATORY POWERS ACT (IPA) 2016

8.1. Part 3 of the Investigatory Powers Act 2003 and associated Codes of Practice govern the acquisition of communications data. The term "communications data" includes the 'who', 'when', 'where' and 'how' of a communication, but not the 'what' (i.e. the content of what was said or written).

8.2. Communication can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services. Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services.

8.3. IPA provides the Authority with the statutory power to obtain communications data from telecommunications operators and/or postal operators only where this is necessary to prevent the death, injury or damage to a person's physical or mental health or to mitigate against any such injury or damage. As with RIPA, any such acquisition must also be necessary, proportionate and avoid collateral intrusion (see paragraphs 4.2 to 4.8 above).

8.4. It should also be noted that the Communications Act 2003 requires certain telecommunications operators to provide communications data to the emergency services following a '999' emergency call. Further details on this are contained in the Public Emergency Communications Service Code of Practice. IPA and the Codes of Practice associated with it are not intended to regulate the handling of an emergency call but to ensure that the boundary between IPA and the Communications Act 2003 (and the Public Emergency Communications Service Code of Practice) is clear. Consequently, a period of one hour after the termination of an emergency call (referred to as "the golden hour") is recognised as falling outside the provisions of IPA in relation to the disclosure of communications data to emergency services.

Process for the Acquisition of Communications Data.

8.5. This features three roles:

1. The Applicant;
2. The Single Point of Contact (SPoC); and
3. The Authorising Individual.

Each of these roles should be carried out by a different person.

The Applicant

8.6. This is the person involved in conducting an investigation or operation who makes the application in writing or electronically for the acquisition of communications data. The application must include all relevant details and address the necessity and proportionality for the proposed acquisition of communications data together with any associated collateral intrusion considerations. Further details on what the application must include can be found in the relevant Code of Practice.

The Single Point of Contact (SPoC)

8.7. The Single Point of Contact (SPoC) is an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between the Authority, the Office for Communications Data Authorisations and telecommunications operators and postal operators. A SPoC is required to complete an appropriate training course and be accredited by the Home Office. Upon accreditation, the Home Office will issue the SPoC with a "unique identifier". This sits alongside the authentication services provided by the Home Office to telecommunications operators and postal operators to validate SPoC credentials.

8.8. The accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for the acquisition of communications data are undertaken. The role of the SPoC is to provide objective judgement to the Authority on any application to acquire communications data and in so doing provides a "guardian and gatekeeper" function ensuring that the Authority acts in an informed and lawful manner.

8.9. The views of a SPoC should be sought on all applications to acquire communications data, prior to the application being submitted. The role of the SPoC is to review, prior to submission, applications to acquire communications data and in so doing to:

(a). assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practicable or whether the specific data is inextricably linked to other data;

(b). advise applicants on the most appropriate methods for obtaining data where the data concerned is processed by more than one telecommunications operator and/or postal operator;

(c). engage with applicants to develop and implement effective strategies to obtain communications data;

(d). advise on and manage the use of the "request filter", specifically in relation to the progress of requests through the filter and compliance by the filter with the relevant authorisation (***NOTE***: the "request filter" is operated by the Home Office and provides an additional safeguard in relation to the acquisition of communications data);

(e). advise on interpretation of IPA, particularly where an authorisation to acquire communications data is appropriate;

(f). provide assurance that applications (or authorisations, as the case may be) are lawful under IPA and free from errors;

(g). consider and where appropriate provide advice on possible unintended consequences of the application or authorisation (as the case may be); and

(h). assess any cost and resource implications for both the Authority and the telecommunication operator or postal operator.

8.10. The view of the SPoC on the above issues must accompany an application for authorisation to acquire communications data.

The Authorising Individual

8.11. IPA provides for the independent authorisation by the Investigatory Powers Commissioner of applications from public authorities for the acquisition of communications data. In practice, authorisations will be granted by staff within the Office for Communications Data Authorisations (OCDA).

8.12. OCDA is responsible for granting non-urgent authorisations.

8.13. Urgent authorisations (see below) are granted by a Senior Designated Officer.

Urgent Authorisations (Written and Oral) – Senior Designated Officer

8.14. IPA also provides, however, that in urgent cases the acquisition of communications data can be authorised by a Senior Designated Officer of the Authority. For this Authority, "urgent" would be where there is an immediate threat of loss or serious harm to human life. Where practicable, the SPoC should still be consulted prior to the urgent authorisation being granted but IPA also provides for the granting of an urgent authorisation without prior consultation with the SPoC in "exceptional circumstances". Such "exceptional circumstances" would also include a threat of loss or serious harm to human life.

8.15. Additionally, where it would not be reasonably practicable to complete a written authorisation process in the time available to meet an operational or investigative need then an application may be made and approved orally. Where an urgent oral authorisation is given, a written notice of this must be provided to the telecommunications operator or postal operator by ***no later than one working day*** after the oral authorisation has been given. Failure to do so constitutes an error reportable to the IPC by the telecommunications operator or postal operator and must also be recorded by the Authority.

8.16. For any urgent authorisation, a written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC must collate details or copies of Control Room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decisions made by the Senior Designated Officer and the actions taken in respect of those decisions. An explanation of why the urgent process was undertaken must also be recorded.

8.17. An urgent authorisation has effect for three days only, beginning with the day on which it was granted. If it is considered that it will still be necessary to acquire communications data after this three day period, then application must be made to and authorisation sought from the OCDA.

8.18. A list of Senior Designated Officers for this Authority for urgent authorisations can be found at Appendix B

Records Retention

8.19. Copies of:

1. all written applications made to the Office for Communications Data Authorisations for authorisation to acquire communications data;
2. all authorisations/rejections of authorisations received from the Office for Communications Data Authorisations; and
3. Any urgent applications and authorisations

must be provided to the RIPA & IPA Co-ordinator, for central retention, at the earliest opportunity.

This page is intentionally left blank