Revision 4 – 28 10 20

Runnymede Borough Council

Investigatory Powers Act 2016

Acquisition of Communications Data Policy

CONTENTS

1. INTRODUCTION

1.1. The Investigatory Powers Act 2016 (IPA 2016) governs how local authorities use the investigatory powers available to them, in relation to the lawful acquisition of Communications Data (CD). The IPA 2016 provides transparency and privacy protection, strengthening existing safeguards and introducing oversight arrangements. It also introduces a new Investigatory Powers Commission (IPCO) to oversee how these powers are used.

1.2. The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allowed the local authorities to obtain CD from Communications Service Providers (CSPs) in connection with criminal investigations.

1.3. The IPA 2016 extends the range of data local authorities are able to request from providers but ensures independent authorisation for the acquisition through the new Office for Communications Data Authorisations (OCDA). However, it continues only to be a justifiable interference with an individual's human rights if such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.

1.4. All applications for CD must be made via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All local authorities must use the National Anti-Fraud Network (NAFN) as their SPoC. Therefore, all applications to access CD will be made through NAFN via their online application service.

1.5. The introduction of OCDA means the acquisition of CD by local authority officers no longer requires judicial approval.

1.6 Runnymede Borough Council (RBC) has appointed what is termed as a Senior Responsible Officer (SRO) whose role is to ensure the integrity of the processes it has in place for acquiring CD and reporting any errors to the IPCO. The SRO for RBC is the Corporate Head of Law and Governance.

1.6. These powers should not be confused with any Policy and practices with regard to monitoring under the lawful business practices legislation. This latter legislation relates to the monitoring of RBC's own communication and computer systems.

2. SCOPE OF POLICY

2.1. This Policy sets out RBC's procedures and approach for obtaining and handling CD for the purposes of preventing or detecting crime or of preventing disorder; the only lawful reasons for RBC staff to use IPA 2016 legislation to access CD.

2.2. This Policy should be read in conjunction with the Communications Data Code of Practice (COP) issued under the IPA 2016. This also creates a system of safeguards, consistent with the requirements of Article 8 (rights to

privacy) of the Human Rights Act 1998. The COP is admissible in evidence in criminal and civil proceedings.

2.3. The COP can be obtained using the link detailed below and is available to all Council staff involved in the acquisition of CD.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf

2.4. Both this Policy and the COP will be followed at all times and under no circumstances should access to CD be sought outside of this guidance.

2.5. RBC will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the objectives of RBC.

3. ROLES OF STAFF INVOLVED IN THE PROCESS

3.1. The process for the acquisition of CD under the IPA 2016 requires the following personnel:

- Applicant
- Approved Rank Officer (ARO)
- Single Point of Contact (SPoC)
- OCDA Authorising Individual

4. APPLICANT

4.1. The Applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of CD. The Applicant completes an application form, setting out for consideration the necessity and proportionality of a specific requirement for acquiring CD. Prior to the completion of the relevant paperwork, it may be advisable for the Applicant to consult with the SPoC at NAFN.

5. APPROVED RANK OFFICER

5.1. The ARO is a person of Service Manager level or equivalent within RBC who confirms to NAFN that they are aware that an application has been made. They do not have any authorising function but are responsible for the integrity of the process in place and the overall quality of that process.

5.2 Current ARO's appointed by RBC are the following post holders:

- Corporate Head of Environmental Services
- Head of Housing Services & Business Planning

6. SINGLE POINT OF CONTACT

6.1. The SPoC is either an accredited individual (passed the Home Office course) or a group of accredited individuals such as the National Anti-Fraud Network, who are trained to facilitate lawful acquisition of CD. All accredited officers are issued a Personal Identification Number (PIN). Details of all accredited

individuals are available to Communication Service Providers (CSPs) for authentication purposes.

6.2. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for CD are undertaken. The SPoC provides objective judgement and advice to the Applicant and provides a "guardian and gatekeeper" function, ensuring that local authorities act in an informed and lawful manner.

6.3. As already explained, RBC can only use the services of NAFN as the its SPoC. Therefore, all applications to access CD will be made through NAFN.

6.4. The SPoC will be in a position to:

- Engage proactively with Applicants to develop strategies to obtain CD and use it effectively in support of operations or investigations;
- Assess whether the acquisition of specific CD from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- Advise Applicants on the most appropriate method for the acquisition of data where the data sought engages a number of CSPs;
- Advise Applicants on the type of data that can be obtained to meet their purposes.
- Provide assurance to AROs that Authorisations and Notices are lawful under the IPA and free from errors;
- Provide assurance to OCDA that an application has been verified and checked.
- Assess whether CD disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;
- Assess whether CD obtained by means of an Authorisation fulfils the requirement of the Authorisation;
- Assess any cost and resource implications to both RBC and the CSP of data requirements.

7. OCDA AUTHORISING INDIVIDUAL

7.1. The OCDA officer receives the application from the NAFN SPoC and checks the application meets the necessary criteria before authorising or rejecting and issuing a Decision Document. NAFN will retain the original of all the documents. These will be retained within the on-line portal. Copies of the documents must be retained by the Applicant, ARO or within the relevant department for inspection by the IPC and for audit, filing and disclosure purposes under the Criminal Procedures Investigation Act 1996. (OCDA will only hold the applications and Decision Documents for a limited period of time due to the degree of sensitivity and risk arising from the accumulation of these documents in a central database).

8. WHAT IS COMMUNICATIONS DATA

8.1. CD does not include the content of any communication. It is not lawfully possible for RBC employees under any circumstances to obtain the content of communications.

8.2. The term ‘CD’ embraces the ‘who’, ‘when’ and ‘where’ of a communication but not the content - not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video.

8.3. CD can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

8.4. CD is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

8.5. Where the provision of a communication service engages a number of providers, the SPoC will determine the most appropriate plan for acquiring the data.

8.6. When enquiries regarding CD are being considered within an investigation, it may be advisable that Applicants seek advice and guidance from the SPoC at NAFN.

9. COMMUNICATIONS DATA DEFINITIONS

9.1. The IPA 2016 introduces new terminology for CD – Entity Data and Events Data

9.2. Entity Data describes the ‘who’ involved in the communication – the subscriber and the links between different entities or communicators. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

9.3. Examples of entity data requests include:

- Subscriber checks, such as who is the subscriber of phone number 01234 567 890?
- Who is the account holder of e-mail account example@example.co.uk?
- Who is entitled to post to web space www.example.co.uk?
- Subscribers’ or account holders’ account information, including names and addresses for installation, and billing including

payment method(s), details of payments e.g. for pre-paid mobiles.

- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services.
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
- Information about selection of preferential numbers or discount calls.

9.4. Event Data identifies or describes events in relation to a telecommunications system which consists of one or more entities engaging in an activity at a specific point or points in time – the 'what, when and where'. For obtaining Event Data there is a Serious Crime Threshold (see 11.1)

9.5. Examples of Event Data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- Itemised telephone call records (numbers called)12;
- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

10. POSTAL DEFINITIONS

10.1. A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose is to make available or facilitate the transmission of postal items containing communications. CD in relation to a postal service is defined at section 262(3) of the IPA 2016 and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to use made by a person of a postal service;
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service.

10.2. Postal data is defined in section 262(4) of the IPA 2016 and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

10.3. In the postal context anything included inside a postal, item, which is in transmission, will be content. Any message written on the outside of a postal item which is in transmission may be content and fall within the scope for the interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning it's routing, for example the address of the recipient, the sender and the postmark, is postal data and will not be content.

11. WEB BROWSING AND COMMUNICATIONS DATA

11.1. Web browser software provides one way for users to access web content. When using a browser to access the web, a user may enter a web address. These are also referred to as uniform resource locators (URLs).

11.2. Some elements of a URL are necessary to route a communication to the intended recipient and are therefore CD. The URL may also contain the port, which is an extended part of the Internet Provider (IP) address and the user information – including usernames and authorisations. The port and user information will be CD.

12. RELEVANT COMMUNICATIONS DATA

12.1. A Data Retention Notice under the IPA 2016 may only require the retention of relevant CD. This is defined at section 87 of the IPA 2016 and is a subset of CD.

It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication;
- The time or duration of a communication;
- The type, method or pattern, or fact of a communication;
- The telecommunication system to or through which a communication is transmitted;
- The location of any such system.

13. INTERNET CONNECTION RECORDS

13.1. An Internet Connection Record (ICR) is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is CD.

13.2. An ICR will only identify the service that a customer has been using. For example many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling RBC to make further enquiries of the social networking provider identified.

13.3. Further detail on the definitions described above and the types of CD that can be accessed is available in the COP.

13.4. The SPoC will provide advice and assistance with regard to the types of data which can be lawfully obtained and how that data may assist an investigation. Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional types of CD may be retained by a telecommunications operator or postal operator for their own business use, the Applicant should discuss this with the SPoC.

14. PREPAID MOBILE PHONES

14.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily. It is possible that a subscriber check will identify a number as belonging to one of these devices. This does not necessarily prevent an investigating officer obtaining useful information. The Applicant can ask for further information about the subscriber under section 21(4)(c) of the IPA 2016, including top-up details, method of payment, the bank account used or customer notes etc.

14.2. So as to allow for the widening of the data capture, the Applicant should outline in their original application that further information will be required if the phone turns out to be prepaid, this information could be requested in two stages. Firstly, asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information.

14.3. The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc. are the third parties involved in the transaction of credit placed on a

mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a Notice under the IPA; instead the data can be applied for under the Data Protection Act 2018 via the SPoC.

15. WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM

15.1. CD can be obtained from a CSP. A CSP is an operator who provides a postal service such as Royal Mail or telecommunications service, such as the usual telephone service providers. However, there may be less obvious companies which may be classed as a CSP. The SPoC at NAFN will determine which CSP they will contact to obtain the data on behalf of the Applicant. However, any intelligence obtained which establishes which CSP may provide the data should be included within the application or by notifying the SPoC.

16. LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA

16.1. As mentioned earlier RBC's only lawful reasons to access CD is for the purpose of preventing or detecting crime or of preventing disorder.

16.2. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

16.3. RBC can only lawfully process and consider applications to access CD on behalf of RBC. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain CD; in these circumstances RBC can only apply for data which it would usually be allowed to access. It should be clear in the investigation documentation that it is a joint investigation as it may have to be justified to a Court or Tribunal.

16.4. RBC staff must not apply on behalf of any third parties who do not have lawful authority to obtain CD. Should an organisation make such an approach this must be reported to the Senior Responsible Officer (SRO) who has the responsibility for the Council's working practices in relation to obtaining CD.

16.5. Where RBC is contracted to undertake work on behalf of a third party, CD may be obtained if RBC is the investigating and prosecuting body.

17. USING OTHER POWERS

17.1. The IPA 2016 is the primary legislation for the acquisition of CD and should always be the first option considered due to the rigorous and independent assessment and authorisation process.

18. INTERNAL INVESTIGATIONS

18.1. The COP state where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Chapter II IPA 2016 to obtain CD for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain CD under the IPA 2016.

18.2. If CD is sought in connection with officers of RBC committing crimes against RBC, it is important that the enquiry is a genuine criminal investigation with a view to proceeding criminally as opposed to just a disciplinary matter. Advice may be required from the Corporate Head of Law and Governance if this arises.

19. SERIOUS CRIME THRESHOLD

19.1. With effect from 1st November 2018 the IPA 2016 introduced a new Serious Crime Threshold to applications for CD. This means that RBC may only acquire Events Data where the crime can be defined as a serious crime. Where the crime cannot be defined as serious, only Entity Data may be obtained.

19.2. The following definitions of serious crime apply:

- An offence that is capable of attracting a prison sentence of 12 months or more;
- An offence by a person who is not an individual (i.e. a corporate body);
- An offence falling within the definition of serious crime in section 263(1) of the IPA 2016 (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose);
- An offence which involves, as an integral part of it, the sending of a communication;
- An offence which involves, as an integral part of it a breach of a person's privacy.

20. NECESSITY AND PROPORTIONALITY

20.1. The COP states the acquisition of CD under the IPA 2016 will be a justifiable interference with an individual's human rights under Article 8 Right to Privacy, only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

20.2. Below is guidance to assist Applicants with factors that impact on necessity and proportionality.

21. NECESSITY

21.1. In order to justify the application is necessary, the Applicant needs as a minimum to consider three main points:

1. The event under investigation, such as a crime or disorder offence;
2. The person, such as a suspect, witness or missing person and how they are linked to the event;
3. The CD, such as a telephone number or IP address, and how this data is related to the person and the event.

21.2. In essence, necessity should be a short explanation of 1) the event, 2) the person and 3) the CD and how these three link together. The application must establish a link between the three aspects to be able to demonstrate the acquisition of CD is necessary for the statutory purpose specified.

21.3. Necessity does not entail explaining ‘what will be achieved by acquiring the data’ or ‘why specific time periods have been requested’, these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

22. PROPORTIONALITY

22.1. Applicants should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

22.2. This outline should include an explanation of how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a phone number may be obtained from online enquiries or other publicly available sources.

22.3. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation. The two basic questions are:

- What are you looking for in the data to be acquired and;
- If the data contains what you are looking for, what will be your next course of action?

22.4. Particular consideration should be given to any periods of days or shorter periods of time which might achieve the objective. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP.

22.5. An explanation as to how CD once acquired will be used, and how it will benefit the investigation or operation will enable the Applicant to set out the basis of proportionality.

22.6. An explanation of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

22.7. An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

23. COLLATERAL INTRUSION

23.1 Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for Events Data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion.

23.2 The question to be asked is 'Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?' For example, itemised billing on the subject's family home will be likely to contain calls made by the family members.

23.3 Applicants should not write about a potential or hypothetical 'error' and if the Applicant cannot identify any meaningful collateral intrusion, that factor should be recorded in the application i.e. 'none identified'.

23.4 It is accepted that for a straight forward subscriber check there will be no meaningful collateral intrusion.

24. THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA

24.1. The legislation provides two different methods of acquiring CD (see below). The SPoC at NAFN will be responsible for deciding the process for obtaining the data required and passing responses from the service provider to the Council.

24.2. The two methods are:

- Authorisation of conduct, or
- Authorisation to give a Notice

24.3. An authorisation of conduct to acquire CD may be appropriate where, for example:

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of CD. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure

accurate and timely acquisition of CD, while maintaining security and an audit trail;

- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the CD.

An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the CD.

25. THE APPLICATION PROCESS

25.1. From April 2019 the IPA 2016 removes the requirement to obtain judicial approval. Applications will only require Independent Authorisation.

25.2. Prior to an Applicant applying for CD, they should contact a SPoC at NAFN who will be in a position to advise them regarding the obtaining and use of CD within their investigation. This will reduce the risk of the Applicant applying for data which they are not able to obtain. It will also assist the Applicant to determine their objectives and apply for the most suitable data for those circumstances.

25.3. RBC will use the automated application process provided by NAFN. This automated service contains the relevant documentation for the Applicant to complete the relevant forms.

25.4. To use the system, Applicants and the ARO have to individually register on the NAFN website - www.nafn.gov.uk. A number of departments within RBC have contributed towards the NAFN annual membership fee; therefore an Applicant needs to confirm with their Line Manager that they are allowed to register.

25.5. With regard to shared services, the local authority on whose behalf the request is being made must be a member of NAFN and the request made via login details for that local authority. Applicants and AROs cannot make use of one local authority's membership to obtain any information on behalf of another. Login details will be necessary for each local authority that an individual is employed by or works on behalf of.

25.6. The online application form, once completed by the Applicant will be forwarded electronically to a SPoC at NAFN who will then perform their responsibilities and if required they will contact the Applicant regarding the contents of the application form. The SPoC at NAFN will obtain confirmation from the nominated ARO that they are aware of the application before proceeding.

25.7. The SPoC confirms that RBC is permitted to use the recorded statutory purpose and determines the conduct to satisfy RBC's need (the type of data that is required). If Event Data is required the SPoC checks the Applicant has recorded a description of the offence(s) and a justification for the seriousness of the offence(s)

25.8. The SPoC can return the application to RBC for a re-work if it does not meet the necessary criteria.

25.9. Once approved the SPoC refers the application to OCDA for authorisation. OCDA then return the application to NAFN for the SPoC to obtain the authorised data from the CSP.

25.10. If the OCDA officer rejects the application it can be returned to the applicant for a re-work.

26. TIME SCALES

26.1. A new Operational Prioritisation has been introduced to enable NAFN to convey to OCDA the operational urgency for the acquisition of data and ensure it is appropriately triaged and handled to meet these demands.

26.2. Operational Prioritisation is categorised in Priority Levels 1-4 and for each Priority rating there is an expected Service response time.

26.3. RBC will generally be submitting requests that are Priority Level 4 – Routine- for which the response should be within 4 working days or 60 working hours.

27. APPLICATION FORM

27.1. The Applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for CD. An application to acquire CD must:

- describe the CD required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the IPA 2016;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the CD relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data
- include the operation name (if applicable) to which the application relates;

28. URGENT ORAL AUTHORISATION

28.1. There is no provision under the IPA 2016 for RBC to orally provide authority to obtain CD. All requests will be made in writing on the NAFN portal and require authorisation from a ARO.

29. ERRORS

29.1. There is a requirement to record or in some instances report to IPCO errors that occur when accessing CD. The thorough checking of operating procedures, including the careful preparation and checking of applications, Notices and Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.

29.2. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of CD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore, the SPoC or other persons involved in the process should bring to the immediate attention of the SRO either a recordable error or a reportable error and the necessary action can then be taken in line with the COP.

29.3. Where material is disclosed by a CSP in error, which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the IPCO has been made.

29.4. An error can only occur after:

- The granting of an Authorisation and the acquisition of data has been initiated, or
- Notice has been given and the Notice has been served on a CSP in writing, electronically or orally.

29.5. It is important to apply the procedures correctly to reduce the risk of an error occurring. Where any error occurs, a record will be kept.

29.6. There are two types of errors:

- Reportable
- Recordable

30. REPORTABLE ERROR

30.1. Where CD is acquired or disclosed wrongly a report must be made to the IPCO. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

30.2. Examples can include:

- An Authorisation or Notice made for a purpose, or for a type of data which the relevant public authority cannot call upon or seek, under the IPA 2016;
- Human error, such as incorrect transposition of information from an application to an Authorisation or Notice;
- Disclosure of the wrong data by a CSP when complying with a Notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an Authorisation;

30.3. Any reportable error must be reported to the SRO as soon as it is identified and then a report will be made to the IPCO within five working days. The report must contain the unique reference number of the Notice and details of the error, plus an explanation how the error occurred and indicate whether any unintended collateral intrusion has taken place. It will also provide an indication of the steps that will take place to prevent a reoccurrence. The 'reporting an error by accredited SPoC form' (CD5) should be used for this purpose.

30.4. If the report relates to an error made by a CSP, RBC must still report it. The CSP should also be notified to enable them to investigate the cause.

31. RECORDABLE ERROR

31.1. 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 RBC and NAFN of such occurrences. These records must be available for inspection by the IPCO.

31.2. The staff involved in the process of acquiring CD must report errors once they have been identified. It will not be acceptable for the error to be ignored.

31.3. Examples can include:

- A Notice given, which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;
- Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or

obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid.

32. EXCESS DATA

32.1. Where authorised conduct results in the acquisition of excess data, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so – for example in relation to a criminal investigation.

32.2. Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 and the IPA 2016 Codes of Practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation.

32.3. If having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The SRO (or a person of equivalent grade or authority) will review the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation.

32.4. As with all CD, the requirements of relevant data protection legislation and data retention policies should be adhered to in relation to excess data.

33. RECORD KEEPING AND SECURITY OF DATA

33.1. All the records and any data obtained must be kept secure and confidential.

33.2. RBC must retain copies of all Applications, as a printed copy of the online application submitted via NAFN, and any other associated documentation where copies have been provided by the NAFN SPoC. This will be coordinated by the RIPA Monitoring Officer who also holds copies of applications for surveillance as per the RBC's RIPA Policy.

33.3. The copy application records must be available for inspection by the IPCO. The IPCO will also be able to obtain copies direct from NAFN.

33.4. The SRO will have access to all of these forms as and when required.

33.5. RBC must also keep a record of the following:

- Number of applications submitted to the NAFN SPoC;
- Number of applications submitted to the NAFN SPoC which were referred back to the Applicant for amendment or declined by the SPoC;
- The reason for any amendments being required or application being declined by the SPoC;
- The reason for any referrals back or rejections;
- Whether any part of the application relates to a person who is member of a profession that handles privileged or otherwise confidential

information (such as a Medical Doctor, Lawyer, Journalist, MP or Minister of Religion (and if so, which profession);

34. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA 1996)

34.1. The Criminal Procedure and Investigations Act 1996 (CPIA 1996) requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor. Therefore, all material relating to the accessing of CD falls under these provisions. If the Applicant is not the Disclosure Officer in the case, they must make the Disclosure Officer aware of all of the material relating to the application and acquisition of the CD.

34.2. All material which may be relevant to the investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence and if prosecuted, at least until the accused is acquitted or convicted, or the prosecutor decides not to proceed with the case and in line with the RBC's Data Retention Policies.

34.3. Where the accused is convicted, the data which is relevant must be retained at least for six months from the date of conviction, and where the court imposes a custodial sentence, until the convicted person is released from custody.

34.4. If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction and in line with the RBC's Data Retention Policies.

35. DATA PROTECTION ACT 2018 (DPA 2018) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

35.1. CD acquired or obtained under the provisions of the IPA 2016, and all copies, extracts and summaries of it must be handled and stored securely in line with the requirements of data protection legislation and regulations.

35.2. There is no provision in the IPA 2016 preventing CSPs from informing individuals about the disclosure of their CD in response to a Subject Access Request. However, a CSP may exercise certain exemptions to the right of subject access. If a CSP receives a Subject Access Request they must carefully consider whether in the particular case, disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

35.3. Should a request for advice be made from a CSP to the SPoC regarding a disclosure, the SPoC will consult with RBC's Data Protection Officer and the Applicant if necessary before a decision is made. Each case should be examined on its own merits.

35.4. Equally, these rules will apply should a Subject Access Request be made from an individual where material under this legislation is held by RBC.

35.5. A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner and the courts etc.

36. OVERSIGHT

36.1. The IPA 2016 provides for the IPCO whose remit includes providing comprehensive oversight of the use of the powers contained within the IPA 2016 and adherence to the practices and processes in the COP. They carry out inspections, and for the purposes of RBC applications, carry out inspections of NAFN. Should they have any concerns regarding an application they would contact the relevant staff involved at RBC. It is possible that they could also inspect RBC.

36.2. It is important to note that should the IPCO establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the IPA 2016 in relation to the acquisition or disclosure of CD, they shall, subject to safeguarding national security, inform the affected individual of the existence of the Investigatory Powers Tribunal and its role. The IPCO should disclose sufficient information to the affected individual to enable him or her to effectively engage the Investigatory Powers Tribunal.

37. COMPLAINTS

37.1. The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the IPA 2016. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner at the following address:

37.2.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

0303 123 1113

www.ico.org.uk

The Investigatory Powers Tribunal has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by the IPA 2016.

The Investigatory Powers Tribunal is an independent body made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint the IPT can undertake its own enquiries and complaints and can demand access to all information necessary. Information regarding the IPT and how to make a complaint can be found at www.ipt-uk.com, or by writing to:

The Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

38. STRATEGY AND POLICY REVIEW

38.1. The Corporate Head of Law and Governance will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of RBC.

Responsible Officer: Corporate Head of Law and Governance

Date: November 2020

Review frequency as required by legislative changes.