New Forest DISTRICT COUNCIL

POLICY FOR THE ACQUISITION OF COMMUNICATIONS DATA

Human Rights Act 1998,

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Investigatory Powers Act 2016

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE CURRENT HOME OFFICE CODE OF PRACTICE: "ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA".

CONTENTS **Page**

1 BACKGROUND

1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.

1.2 Article 8 of the Convention reads as follows: -

"Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others."

1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person's right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.

1.4 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework whereby certain investigations can be carried out in a lawful, regulated and proportionate manner so that an individual's Article 8 rights are not infringed.

1.5 This Policy is concerned with the provision in RIPA enabling certain communications data to be acquired by public authorities in a manner which is compatible with Article 8. This Policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any acquisition of communications data is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA. (The Council has a separate Surveillance Policy which deals with Directed Surveillance and Covert Human Intelligence Sources).

1.6 The acquisition of communications data can **only** be authorised by the Council under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime** or for the **prevention of disorder**.

1.7 All officers who apply for communications data to be obtained or disclosed should be familiar with RIPA, this Policy, and the Home Office "Code of Practice for the Acquisition and Disclosure of Communications Data" which can be found at https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data.

1.8 Acquiring communications data without authorisation or outside the scope of an authorisation will mean that the "protective umbrella" of RIPA is unavailable, and could expose the Council to the risk of legal action. It may also result in disciplinary action being taken against the officer/officers involved.

2 NATIONAL ANTI-FRAUD NETWORK

2.1 The Council uses the National Anti-Fraud Network ("NAFN") to deal with all applications for the acquisition of communications data. The application process, and NAFN's role in this process, is detailed below under "Applications and Authorisations".

2.2 NAFN provides a service whereby all applications are checked by an accredited individual (a "Single Point of Contact" or "SPoC") to ensure compliance with RIPA. NAFN has direct access to the databases of a number of Communications Service Providers ("CSPs"). This means that if an authorisation is granted to allow a person to engage in conduct required to obtain communications data (see paragraph 4.1.1 below), and NAFN has access to the database of the relevant CSP, the NAFN SPoC will be able to obtain that data directly.

2.3 In order to access the NAFN secure website to make an application for communications data, an Applicant will require a username, password and PIN.

2.4 Should a manager consider that it is necessary for a Council employee to use the NAFN secure website to make applications for communications data, this must be authorised in writing by the employee's Service Manager. Where the Service Manager has provided their authorisation, the manager should notify NAFN of the details of the employee who requires log in details for the system.

3 WHAT TYPES OF DATA CAN BE ACQUIRED?

3.1 "Communications data" is generated, held or obtained by CSPs and may relate to use of the following services:-

3.1.1 Postal service

3.1.2 Email

3.1.3 Landline telephone

3.1.4 Mobile telephone

3.1.5 Internet

3.2 Local authorities may **NOT** acquire any information about the content of communications (eg, what was said, or what data was passed on), or the location of a mobile device used to make a call.

3.3 Local authorities may acquire communications data of the following types: -

3.3.1 **'Service use information'**. This is information about the services provided to an individual. It will include information about:

a) the use made by any person of any postal service or communications service;

b) the use made by any person of any part of a telecommunications system, in connection with the provision to or use of any telecommunications service.

Service information might include, for example, information regarding itemised billing (numbers called, timing and duration of service usage), use of call diversions/forwarding, itemised records of connections to internet services, information about amounts of data downloaded or uploaded, information about selection of preferential numbers or discount calls, records of registered post and parcel consignment.

3.3.2 **'Subscriber information'**. This is information about the person who uses a service. It will include any information held by the provider of a postal or telecommunications service, regarding the persons to whom they provide the service.

This might include subscriber details, including names, addresses and other customer information, for example, the identity of the subscriber to telephone number 01234 567891, or email address example@example.co.uk, or who is entitled to post to web space www.example.co.uk.

3.4 The above examples are not exhaustive lists of the communications data which may be acquired. If officers are in any doubt about the types of data which they may be able to acquire, or the ways in which this might be acquired, they should seek advice from a SPoC (see paragraph 5.3 below).

3.5 Applicants and Designated Persons (see paragraph 5.4 below) should bear in mind that it may be appropriate to obtain subscriber information (ie, to check that the person who subscribes to a service is a person relating to their investigation) before they can determine whether it is necessary and proportionate to go on to acquire service use information, such as itemised billing.

4 AUTHORISATIONS AND NOTICES

4.1 Communications data can be acquired in two ways: by Authorisation or by Notice:

4.1.1 An Authorisation enables the authorised person (generally the SPoC) to engage in conduct required to obtain the communications data;

4.1.2 A Notice requires a CSP to disclose the data in their possession, or to obtain and disclose the data.

4.2 The SPoC will be able to advise which of these methods will be most appropriate in relation to a particular investigation. In the majority of cases, the Council will use an Authorisation, authorising the SPoC to obtain the data required from the relevant CSP.

5 DIFFERENT ROLES

5.1 There are four key roles relevant to the acquisition of communications data:

- Applicant
- Single Point of Contact (SPoC)
- Designated Person
- Senior Responsible Officer

5.2 **Applicant**

The Applicant will generally be the investigating officer, who will complete the application form, setting out for consideration by the Designated Person the necessity and proportionality of acquiring the communications data.

5.3 **Single point of contact**

A SPoC must have formal accreditation, and is trained to facilitate the lawful acquisition of communications data and effective cooperation between a public authority and CSPs. In this way, the SPoC provides a "guardian and gatekeeper" function. The SPoC provides objective judgement and advice to both the Applicant and Designated Person.

The Council does not have an internal Single Point of Contact (SPoC), but uses the SPoCs at NAFN, who hold the necessary accreditation.

5.4 **Designated Person**

The Designated Person is the person within the Council who reviews the application and authorises the grant of an Authorisation, or the giving of a Notice, where they consider the acquisition to be necessary and proportionate.

Designated Persons must be independent from the operation or investigation to which the application relates, ie, they should have had no prior involvement with the operation or investigation. If the Designated Person is an Executive Head, they should not authorise applications from within their own Services.

In an exceptional, urgent situation (for example, if there is an immediate threat to life, or an urgent operational requirement for the prevention or detection of serious crime), if there is no independent Designated Person available, the involvement of a non-independent Designated Person must be recorded, and the justification for their involvement explained in their recorded considerations. The involvement of a non-independent Designated Person must be reported to the Commissioner at their next inspection, and the details and reasons may be published by the Commissioner.

The Council's Designated Persons are currently the Chief Executive and Executive Heads.

5.5 **Senior Responsible Officer**

The Senior Responsible Officer is responsible for: -

5.5.1 Ensuring the integrity of the processes in place within the authority to acquire communications data;

5.5.2 Ensuring compliance with RIPA and with the Code of Practice;

5.5.3 Oversight of the reporting of errors to the Investigatory Powers Commissioner's Office (IPCO), the identification of the reasons for the errors, and the implementation of processes to minimise repetition of errors;

5.5.4 Engagement with IPCO inspectors, and oversight of the implementation of any post-inspection plans.

The Council's Senior Responsible Officer is currently the Chief Executive.

6 NECESSITY AND PROPORTIONALITY

The obtaining or disclosure of communications data (by Authorisation or Notice) should only be authorised if the Designated Person is satisfied that:

6.1 The action is **NECESSARY** for the prevention or detection of crime or the prevention of disorder. An application should cover three main points, and should demonstrate the link between these three aspects:

- The event under investigation (ie, the crime or disorder);
- the person (eg, the suspect) and how they are linked to the event; and
- the communications data, and how this relates to the person and the event.

6.2 The action is **PROPORTIONATE.** It should: -

6.2.1 be no more than is required in the circumstances;

6.2.2 impinge as little as possible on the rights and freedoms of the individual concerned and of innocent third parties;

6.2.3 be carefully designed to meet the objectives in question;

6.2.4 not be arbitrary, unfair or based on irrational considerations.

7 APPLICATIONS AND AUTHORISATIONS

7.1 APPLICATION FORM

7.1.1 The Applicant must complete the NAFN application form, which is a standard form approved by the Home Office. As the Council uses the NAFN application process, the Applicant will access the application form by logging onto the NAFN website using their username, password and PIN.

7.1.2 The Applicant should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout

of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality".

7.1.3 The application form must include the following information: -

i) name, rank and position of the Applicant;

ii) a unique reference number (which will be generated automatically by the NAFN website);

iii) the operation name, if applicable;

iv) specify that the communications data is required in connection with the purpose of **preventing or detecting crime or disorder**;

v) describe the communications data required, specifying the time periods for which the data is sought, including (where relevant) any historic or future dates. Any time period specified should be the shortest period in which the objective for which the data is sought can be achieved;

vi) describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

vii) explain why the acquisition of the communications data is **necessary** and **proportionate** (see paragraph 6 above);

viii) consider and, where appropriate, describe any collateral intrusion (ie, explain the extent to which the privacy of an individual not under investigation may be infringed, and why that infringement is justified in the circumstances);

ix) consider and, where appropriate, describe any potential unintended consequences of the application;

x) identify and explain the timescale within which the data is required.

7.2 SPoC REVIEW

7.2.1 Once the Applicant has completed the application form, this must be submitted electronically to the SPoC, who will check that the application is compliant with RIPA, that the acquisition intended is practical and lawful, and that the tests of proportionality and necessity have been properly considered and detailed.

7.2.2 If the SPoC considers that there are any problems with the application, or that further information is required, he will provide advice to the Applicant about the application. This may include, for example, advice about whether it is lawful, possible, or practical to obtain communications data of the nature sought by the applicant, and whether the tests of necessity and proportionality have been properly applied and explained. Where appropriate, the Applicant can make amendments to the application, and can re-submit the application to the SPoC.

7.2.3 Once the SPoC is satisfied with the application, he will complete the relevant sections of the application form, identifying the data to be acquired, and how it may be acquired. The SPoC will then notify the Designated Persons at the Council by email that there is an application pending which requires review.

7.3 AUTHORISATION BY DESIGNATED PERSON

7.3.1 The Designated Person must review the application in detail, before deciding whether to: -

a) authorise the application;

b) reject the application;

c) request further information.

7.3.2 Before deciding whether to authorise an application, the Designated Person should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality".

7.3.3 The Designated Person should consider the proportionality and necessity of the Authorisation/Notice applied for (see paragraph 6 above), and the potential for collateral intrusion. The Designated Person should not simply "rubber stamp" the application. Their reasons for authorising/declining the application should be clear and detailed, and demonstrate that they have considered the substantive merits of the application. If the Designated Person requires further information in order to decide whether to approve an application, they should notify the SPoC that more information is required.

7.3.4 The standard form requires the Designated Person to tick a box to confirm whether they are authorising a person to engage in conduct to acquire communications data, or whether they are authorising a Notice to be served on a CSP, requiring them to obtain/disclose data. The Notice or Authorisation documents themselves will be completed by the SPoC.

7.3.5 The authorised or rejected Application is then submitted back to the SPOC via the NAFN secure website.

8 JUDICIAL APPROVAL

8.1 From 1 November 2012 a person may not engage in the conduct authorised, or serve a Notice on a CSP requiring them to provide communications data, unless and until the Authorisation/Notice has been approved by a Justice of the Peace.

8.2 Before approving an Authorisation or Notice, a Justice of the Peace must be satisfied that: -

At the time of granting the Authorisation, or giving the Notice: -

i) There were reasonable grounds for believing that the Authorisation/Notice was necessary and proportionate;

ii) The person who granted the Authorisation/Notice was an appropriate Designated Person; and

iii) At the time when the Justice of the Peace is considering the matter, there remain reasonable grounds for believing that the Authorisation/Notice is necessary and proportionate.

8.3 The procedure for obtaining judicial approval is as follows: -

i) After the Designated Person has completed the authorisation on the NAFN secure website, NAFN will send an application pack to the Applicant;

ii) The application pack should be forwarded to the Legal Services Manager;

iii) A member of Legal Services will prepare the Magistrates' Court application, and will represent the Council at the Magistrates' Court hearing. The Applicant may be asked to prepare a witness statement and may be required to attend the hearing;

iv) If the Authorisation/Notice is approved, Legal Services will pass the approval to the Applicant. The Applicant will then liaise with the SPoC who will obtain the communications data from the CSP.

v) If the Authorisation/Notice is not approved, or is quashed by a Justice of the Peace, Legal Services will inform the Applicant. The Applicant must inform the SPOC and Designated Person that the Authorisation/Notice was not approved, or was quashed.

8.4 **No action may be taken under the Authorisation or Notice unless and until it has been approved by a Justice of the Peace.**

9 DATA PROTECTION AND HANDLING THE DATA ACQUIRED

9.1 When the communications data has been acquired, it will be made available to the Applicant on the NAFN secure website.

9.2 Information collected through acquisition of communications data may include personal data. It is the responsibility of the Applicant to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Council's Data Protection Policy, Law Enforcement (Data Protection) Policy and the Protection of Special Category Data Policy . In particular, the information obtained must be handled and stored securely. Any queries regarding an officer's obligations under the Data Protection Act or the GDPR should be directed to the Council's Data Protection Officer. .

10 DURATION, RENEWAL AND CANCELLATION

Duration

10.1 All Authorisations and Notices should specify the time period in relation to which the communications data are to be obtained. For example, it might authorise the SPOC to obtain information regarding all calls made from a specified number to another specified number in the two weeks immediately following the Authorisation. Or a Notice might require a CSP to confirm the subscriber details for a specific email account between two specified dates in the past. An authorisation: -

10.1.1 Cannot authorise or require any data to be obtained more than one month after the Authorisation or Notice is granted; and

10.1.2 In the case of a Notice, cannot authorise or require any disclosure of data not already in the possession of the CSP after the end of one month from the date of the grant of the Notice or Authorisation.

Renewal

10.2 RIPA provides that an Authorisation or Notice may be renewed 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.

10.3 Where the Applicant believes that a renewal is necessary and proportionate, they should complete an addendum to the original application, setting out their reasons for seeking renewal. They should then submit this to the SPoC, who will review it in the same way as a new application. Once the SPoC is happy with the application for renewal, they will notify the Designated Person that an application requires review.

10.4 Where a Designated Person is granting a further Authorisation or giving a further Notice to renew an earlier Authorisation or Notice, they should: -

10.4.1 consider and record in writing the reasons that it is necessary and proportionate to continue with the acquisition of the data being generated; and

10.4.2 record the date (and where appropriate the time) when the Authorisation or Notice is renewed.

10.5 A renewal **must** be approved by a Justice of the Peace before it will take effect. Any renewal must therefore be submitted to the SPOC in plenty of time to enable it to be reviewed and forwarded to the Designated Person for approval, and for approval to be sought from a Justice of the Peace. Where a renewal has been approved by a Designated Person, Legal Services must be notified at least **seven** working days before expiry of the original Authorisation or Notice, so that they have sufficient time to seek approval from a Justice of the Peace.

10.6 In practice, given the requirement to obtain the approval of a Justice of the Peace and the time constraints this imposes, it will often be more practical to begin a new application, rather than to renew an existing Authorisation or Notice. Applicants who have not obtained, or do not expect to obtain, the data required within one

month of grant of the Authorisation or Notice should discuss with the SPoC the best way to deal with this.

Cancellation

10.7 Where a Notice has been given to a CSP, and a Designated Person determines that it is no longer necessary or proportionate for the CSP to comply with the Notice, the Designated Person shall cancel the Notice,, and must ensure that the CSP is notified of the cancellation.

10.8 Where an Authorisation has been given and a Designated Person determines that it should cease to have effect because the conduct authorised is no longer necessary or proportionate, the Designated Person shall withdraw the Authorisation, and inform the person authorised by the Authorisation of the withdrawal.

10.9 The cancellation or withdrawal must: -

10.9.1 be in writing;

10.9.2 identify, by reference to its unique reference number, the Notice or Authorisation being cancelled;

10.9.3 record the date (and, where appropriate the time) when the Notice or Authorisation was cancelled;

10.9.4 record the name, office and rank/position held by the Designated Person.

10.10 Normally, it will be the Applicant who realises that a Notice or Authorisation is no longer necessary or proportionate (for example, because they have obtained the information required from elsewhere, or because the investigation has concluded for some reason). In this situation, the Applicant should notify the SPoC immediately. The SPoC will then alert the Designated Person that the Authorisation or Notice should be cancelled. The Designated Person should log on to the NAFN secure website to cancel the Authorisation or Notice. Where necessary, the SPoC will notify the CSP that the Authorisation or Notice has been cancelled.

10.11 Where the Designated Person who authorised the Application is unavailable, one of the other Designated Persons should cancel or withdraw the Authorisation or Notice so that no undue delay is caused.

11 RECORD KEEPING

NAFN keeps a full, electronic record of all applications on the Council's behalf, in accordance with the requirements of RIPA.

12 ERRORS

12.1 Where an error occurs in the grant of an Authorisation, the giving of a Notice, or as a consequence of any authorised conduct, or conduct undertaken to comply with a Notice, a record must be kept.

12.2 There are two types of error: -

i) an error which results in communications data being wrongly acquired or disclosed. This type of error is known as a "Reportable Error".

ii) an error which is identified after the Authorisation or Notice is given, but without data being wrongly obtained or disclosed. This type of error is known as a "Recordable Error".

12.3 If an Applicant or Designated Person identifies a Reportable or Recordable Error, they must notify the SPoC immediately.

12.4 A Reportable Error must be reported to the IPCO. This report will be made by the SPoC at NAFN. It is **essential** that the Council's Senior Responsible Officer and the SPoC is informed about any Reportable Error **immediately**, as the error must be investigated, the facts ascertained and the report made to the IPCO within five working days of discovery of the error. If a SPoC requests assistance from the Applicant or another Council officer in connection with the investigation of an error, all reasonable assistance should be provided promptly.

12.5 If the Council receives material from a CSP which has no relevance to any investigation or operation by the Council, the material should be securely destroyed as soon as the report to the IPCO has been made.

12.6 A record of all Recordable Errors will be held by NAFN, and made available for inspection by the IPCO on request. The record will contain details of the error, how the error occurred, and an indication of what steps have been or will be taken to prevent the error from occurring again. The SPoC will notify the Designated Person and the Council's Senior Responsible Officer of all Recordable and Reportable Errors.

13 POLICY AND IMPLEMENTATION

13.1 The Policy is operational from 15 January 2019 and replaces any previous policies and procedures relating to the acquisition of communications data.

13.2 The Legal Services Manager will report to the Audit Committee annually regarding the use made by the Council of its powers under RIPA.