REPORT TO THE EXECUTIVE

Report No.12

Date of Meeting	**31st August 2006**
Title of Report	**Regulation of Investigatory Powers Act 2000 - Revised Policy**
Portfolio	**Leader**
Link to Corporate Priorities	The powers available to the Council under RIPA can be used in investigations for the prevention or detection of crime. They are linked, therefore to the corporate aim of safeguarding and enhancing the assets and resources of North Wiltshire and the wider community
Key Decision	NO
Executive Workplan Ref	Not Applicable
Public Report	YES

Summary of Report

This report seeks approval for a revised policy and procedures on the exercise of the Council's powers under the Regulation of Investigatory Powers Act 2000 (RIPA) and confirms the designation of appropriate officers in connection with the accessing of communications data under RIPA.

Officer Recommendations

1. **Approve the revised policy and guidelines for the exercise of the Council's powers under RIPA, as attached as Appendix 1 to this report.**
2. **Authorise the appropriate Team Leader to act as 'Designated Person' in respect of the necessary authorisations for accessing communications data (including cancellations and renewals of such authorisations) in accordance with the requirements of the Regulation of Investigatory Powers Act 2000, and the Codes made thereunder except where 3 below applies.**
3. **In cases where the Team Leader is directly involved in the operation of a particular investigation, any such authorisations are to be granted, renewed or cancelled by the appropriate Strategic Manager for the Team concerned, (except in the case where urgent action is required and the appropriate Strategic Manager is not available, in which case another Strategic Manager may authorise).**
4. **Approve the designation of Jane Hales, Investigations Officer as the Council's Single Point of Contact officer for the purposes of accessing communications data under RIPA.**
5. **Delegate authority to the Chief Executive to designate the Council's Single Point of Contact from time to time as the need arises.**

Other than those implications agreed with the relevant Officers and referred to below, there are no other implications associated with this report.

Financial Implications	Legal Implications	Community & Environmental Implications	Human Resources Implications	Equality & Diversity Implications
NONE	YES	NONE	NONE	YES

Contact Officer	Paul Taylor, Solicitor 01249 706598 ptaylor@northwilts.co.uk

1. Introduction

1.1. The Regulation of Investigatory Powers Act 2000 (RIPA) was introduced to provide a framework whereby certain investigatory activities could lawfully be carried out by public authorities in compliance with the Human Rights Act 1998. Where public bodies, including local authorities, wished to carry out covert surveillance or use covert human intelligence sources as part of their investigatory work, they needed to have in place an authorisation procedure for such activities. The purpose of the authorisation procedure was to ensure that these covert activities were only undertaken where it could be shown that they were necessary, proportionate and non-discriminatory.

1.2. In November 2001 the Executive approved a policy and guidelines which set out how the Council would exercise its powers under RIPA . Team Leaders were designated as authorising officers for covert surveillance and the use of covert human intelligence sources (CHIS). At that time, those were the only activities that local authorities could undertake under RIPA. To date, three authorisations have been granted, for specific operations involving licensing and environmental protection investigations.

1.3. It is now appropriate to revise the Council's policy and guidelines for two main reasons. Firstly, the original policy is now some five years old and a number of minor changes are necessary in light of experience and advice from the Office of Surveillance commissioners, which is the body that oversees the use of RIPA by all public authorities. Secondly, and more significantly, the Council can now avail itself of some of the powers in RIPA relating to the accessing of communications data and this needs to be reflected in the policy

2. Accessing Communications Data

2.1 When investigating criminal offences, local authorities can now have limited access to communications data. This is data held by telecommunications or postal service providers about the use of their services by the person under investigation. This data can only be accessed where it is necessary for the prevention or detection of crime and where it has been properly authorised.

2.2 Two types of communications data may be obtained using these powers. Firstly, 'subscriber data', which is information or account details that the service provider may hold relating to the person under investigation. Secondly, the Council can seek access to 'Service data', which is information held by the provider about the use of the communications service by the person concerned – e.g. itemised telephone bills. The Council cannot access the actual contents of communications made.

2.3 The revised RIPA policy and guidance attached as Appendix 1 has been amended to include arrangements for accessing communications data.

3. Authorisations

3.1 As with the other powers under RIPA, there is a requirement to have an authorisation procedure. Authorisations are granted by ' Designated Persons', and it is appropriate to designate Team Leaders to act as Designated Persons, in line with the existing authorisations under RIPA for covert surveillance. In addition, all requests for access to communications data should be made through a designated single point of contact (SPOC). The role of the SPOC is to assess whether it is reasonably practical to obtain the communications data requested, to advise on the types of such data that can be obtained, to check authorisations and to liaise with service providers as appropriate.

3.2 Any person designated as a SPOC must have attended an accredited course and have a PIN reference that is given to service providers when a request s made.

3.3 It is likely that only limited use would be made by the Council of the powers available to it to access communications data. The one area where use may be made of these powers is in connection with benefit fraud investigations. One member of the Investigations Team, Jane Hales, has obtained the necessary accreditation to act as a SPOC and it would be appropriate to confirm her designation as the Council's SPOC.

4. Options and Options Appraisal

4.1 The Council does have the option to appoint a single 'Designated Person' to authorise access to communications data. However, it is considered preferable to authorise all Team Leaders to act in this capacity, both to bring the procedures in line with those for other RIPA authorisations and to ensure that those considering granting authorisations have an understanding of the relevant investigations being carried out.

5. Legal Implications

5.1 The legal implications are set out in the report.

6. Equality & Diversity Implications

6.1 The proper application of the requirements of RIPA should help ensure that any surveillance is carried out in a non-discriminatory manner

7. Risk Analysis

7.1 If the Council were not to appoint any officers to act as Designated Persons and SPOCs, then it would not be able lawfully to access any communications data as part of any investigation. This could hamper such investigations and would lead to criticism from the relevant Inspection authority. Likewise, if the Council were not to update its RIPA policy, it would also be liable to criticism from the Office of Surveillance Commissioners.

Appendices:	1. Regulation of Investigatory Powers Act 2000 - Guidance and Procedure Notes.
Background Documents Used in the Preparation of this Report:	• None

Previous Decisions Connected with this Report

Report	Committee & Date	Minute Reference
Regulation of Investigatory Powers Act 2000	Executive – 22 November 2001	E139