Draft - Regulation of Investigatory Powers Act 2000 (RIPA) Policy

1.0 Extent

1.1 This policy explains how Dorset Council will comply with RIPA when authorising directed surveillance under Section 28(1) of RIPA, covert human intelligence sources under Section 29(1) of RIPA and obtaining communications data under Section 22(3) and 22(4) of RIPA.

1.2 This Policy is supplementary to the relevant provisions of any code of practice issued under RIPA (see https://www.gov.uk/government/collections/ripa-codes).

2.0 Safeguards

2.1 The Council will apply a presumption in favour of overt investigation methods. So, the Council will always look to investigate matters using a variety of overt investigatory tools, before considering whether the use of these powers is required. Directed surveillance, using covert human intelligence sources or obtaining communications data (collectively described in this policy as "covert surveillance") will be used only when other reasonable options have been considered, and ruled out.

2.2 The Council will use covert surveillance proportionately. So, the Council will not use covert surveillance to address minor matters, but instead will focus on those issues which are of greatest concern to the community, so, the Council will:

(a) balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence, or disorder;

(b) explain how and why the methods to be adopted will cause the least possible intrusion on the target and others; and

(c) evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

2.3 Without prejudice to paragraph 2.2 no authorisation for the carrying out of directed surveillance will be granted unless the authorisation is "necessary" for the purposes of preventing or detecting crime and in the case of directed surveillance a crime punishable by a maximum term of at least 6 months imprisonment or for the purpose of preventing or detecting certain other specified offences.

2.4 The Council will only use covert surveillance either to obtain evidence that can be presented at court, or where another positive outcome relating to the prevention or detection of crime has been identified, for example through the positive identification of perpetrators.

2.5 In addition, the interception of Council telecommunications will only be carried out in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and following procedures agreed by the Corporate Director – Legal and Democratic Services in the following circumstances:

- to establish the existence of facts or to ascertain compliance with regulatory or self-regulatory practices (e.g. to keep records of communications where the specific facts are important);
- to check the standards are being achieved or ought to be achieved;
- to prevent or detect crime (e.g. to check that employees or others are not involved in defrauding the Council);
- to investigate or detect unauthorised use of the telecommunications system; or
- to ensure the security of the system and its effective operation.

2.6 The use of internet and social networking sites may be covert surveillance if used to gather evidence or monitoring an individual's status by viewing more than once and will only be carried out once a RIPA authorisation is in place.

3.0 **Responsibilities**

3.1 **The Chief Executive** is the senior responsible officer, who is responsible for:

- Maintaining the integrity of RIPA processes within the Council;
- ensuring compliance with the relevant provisions of RIPA and the codes of practice; and
- engaging with the Investigatory Powers Commissioner's Office and overseeing the implementation of post-inspection action plans.

3.2 The Council will ensure that authorising officers are at Service Manager level as a minimum except where there is the likelihood of confidential information being obtained, when authorising officers will be at Corporate Director level as a minimum. This will avoid any perception that authorising officers are directly involved with the investigations they authorise. Authorising officers will therefore be able to apply more independently reasoned judgment of the issues. No authorisations will be carried out until an order has been made by a Magistrates Court approving that authorisation.

3.3 The **Executive Directors** are responsible for:

- ensuring all applicants for authorisations and authorising officers within their service areas are aware of and trained in RIPA;

- ensuring authorising officers within their service areas meet the standards required by the Investigatory Powers Commissioner's Office.

3.4 The **Corporate Director – Legal and Democratic Services** will be the RIPA co-ordinating officer and is responsible for:

- maintaining a central record of authorisations and collate the original applications/authorisations, reviews, renewals and cancellations; and

- monitoring the quality of notices and authorisations.

3.5 **All officers engaged in covert surveillance** will:

- be familiar with RIPA, the relevant codes of practice and the Investigatory Powers Commissioner's Office procedures and guidance;

- provide the authorising officer with all the information necessary for an informed decision to be made as to whether an authorisation should be granted or cancelled;

- advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance; and

- cease the use of covert surveillance when it no longer meets the authorization criteria.

3.6 The Council's procedures will be set out in a manual available to applicants for authorisations, authorising officers, and the senior responsible officer.

4.0 **Review**

4.1 The Audit and Governance Committee will review this policy and consider a report on the Council's use of RIPA powers annually.