PROTOCOL FOR COVERT INTERNET PROFILE USE - PRINCIPLES

All Covert Internet Profiles must be reported to Legal Services and entered on to their Central Record of Internet Profiles (see Annex 1). This record chronicles the Profile name, date of creation, and the Department and officer responsible for its use (Responsible Officer – RO).

The use of CIPS will be governed by the Principles outlined below:

Principle 1

Use of a covert internet profile (CIP) must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

Principle 2

If a service team wish to use the CIP for covert **monitoring**, then a separate RIPA application must be completed and lodged referring to the intended use of that CIP and this would be approved in accordance with RIPA policy and be captured on the central register through the authorisation procedure.

Principle 3

The use of CIPs for day to day queries, analogous to a car "drive-by", would not fall within the definition of "monitoring" and would not require a formal RIPA authorisation. However, Officers should still satisfy themselves as to necessity and proportionality and ensure that data protection principles are maintained, and the RO should be satisfied as to this justification before approving the officer with their team using the profile. The RO should maintain an appropriate log each time a CIP is used in this regard. The RO will make available upon the request of the Council's RIPA Senior Responsible officer a copy of an up to date log.

Principle 4

The use of a CIP must take into account its effect on individuals and their privacy, with regular reviews (annual) by the RO to ensure maintenance of the profile by the Council remains justified. The RO shall confirm the outcome of that review to the RIPA Senior Responsible Officer for noting in the RIPA central register.

Principle 5

There must be clear responsibility and accountability for CIP profile use including for information collected, held and used.

Principle 6

The duties of the CIP Responsible Officer shall be performed personally. Where they are unable to act owing to absence, illness or operational reasons, the duties shall be performed personally by such member of their staff as has for the time being been nominated deputy for the purposes of this section.

Principle 7

There must be good management, control and monitoring of CIPs. Clear rules, policies and procedures must be in place before a CIP is used, and these must be communicated to all who need to comply with them.

PROTOCOL FOR COVERT INTERNET PROFILE USE - PRINCIPLES

Principle 8

There should be effective review and audit mechanisms to ensure legal requirements and policies are complied with in practice.

Principle 9

A CIP must only be used in pursuit of a legitimate aim and when there is a pressing need for its use. It should then be used in the most effective way to support public safety, with the aim of providing and processing information of evidential value in accordance with data protection principles.

ANNEX 1

RECORD OF COVERT INTERNET PROFILES

Covert Profile Name and Social Media site	When created	Department Profile Held by	Officer Responsible for oversight of profile (RO)	Comments

ANNEX 1

RECORD OF COVERT INTERNET PROFILES
