Addendum to the Public Health Enforcement Policy

6.4 Surveillance and Human Sources including Regulation of Investigatory Powers Act (RIPA)

6.4.1 The Council is a public authority for the purposes of the Human Rights Act 1998. Where an investigation into the prevention or detection of crime and/or prevention of disorder is necessary, for example, following a serious incident or repeat complaints, officers will endeavour to carry out the investigation using overt methods, unless the only means of effective investigation is by way of covert directed surveillance and/or using covert human information sources.

6.4.2 Where we undertake overt surveillance including the use of recording and sampling equipment we will ensure notice is provided to those alleged to be the source of the complaint being investigated informing them of our intentions. Such notice will be no less than 24-hours before surveillance commences which may then be undertaken of over a period of up to six-months before further notice is given if required.

6.4.3 Any covert directed surveillance must be carried out in accordance with Council procedures, RIPA (Regulation of Investigatory Powers Act 2000) and The Protection of Freedoms Act 2012. Authorisation for this type of pre-planned investigation may only be given in writing by formally appointed Authorised Officers (AO) within the Council and before being formally authorised by a Justice of the Peace (JP).

6.4.4 Officers should be mindful that in certain circumstances conducting Open Source Research (OSR) for the purpose of gathering enforcement intelligence i.e. viewing web pages, social networks, chat rooms, information networks (e.g. twitter) and/or web based electronic mail may constitute covert directed surveillance and therefore a RIPA authorisation must be considered. Particular attention will be given to repeat visits to obtain/check or review publically available information in addition to more in-depth research including where profiles/personas are created to gain access to networking sites. Any interaction with other users including making/accepting friends requests, 'poking' or commenting on post will require authorisation.

6.4.5 Where OSR is carried out under a RIPA authorisation then officers are required to complete an Open Source Log/Register including details of any profile/persona used.

6.4.6 The use of any Covert Human Information Sources (CHIS) must also be a carried out in accordance with Council procedures and RIPA. As with directed surveillance, authorisation for this type of information source may only be given in writing by a formally appointed AO within the Council and before being formally authorised by a JP.

6.4.7 A CHIS authorisation is likely to be required where an officer (the handler) establishes or maintains a personal or business relationship with a person for the covert purpose of providing, disclosing or maintaining access to information i.e. if an officer induces, tasks or instructs someone to obtain information.

6.4.8 For further clarification, a CHIS is not someone who volunteers/provides information having no expectation of reward or advantage that has been received by them in the normal course of their life, including through trade/business or normal business practices. In order to remain outside the scope of CHIS, it is essential that no officer attempts to direct that person to carry out any action which would develop or enhance that information.

6.4.9 Any officer considering obtaining any authorisation under RIPA must review and agree this in principle with the Service Manager or Head of Service before submitting the application to the Authorised Officer. In the case of CHIS, the Service Manager or other appointed person must act as the controller and ideally be qualified as a Covert Operations Manager (COM).

6.4.10 The role of the COM as a controller is to be responsible for the management of handlers. They will also have general oversight for the application of CHIS.

6.4.11 The role of a handler is to have day-to-day responsibility for dealing with and directing a CHIS, recording the information supplied and monitoring the CHIS's security and welfare. Any concerns must be brought to the attention of the COM and in turn the AO.

6.4.12 The role of the AO is to be wholly independent of the unit. The AO will risk assess and consider if the criteria set out in 6.4.14 below has been met. They will also be responsible for reviewing and considering subsequent renewals of the authorisation. Further guidelines for AO's are available separately.

6.4.13 A CHIS will only be authorised for a vulnerable person or minor (under 18) in exceptional circumstances. A minor under 16 will never be authorised to provide information against his or her parents/persons with parental responsibility.

6.4.14 Any application under RIPA made by the unit must in general meet the following minimum criteria:

- Be required for prevention and detection of crime only
- In the case of directed surveillance, meet the crime threshold (an offence for which the maximum sentence is 6 months + or where an offence involves the sale of alcohol to a minor)
- In the case of CHIS, adequately consider use (what is being asked), conduct (how it gets done/clear boundaries of action) in addition to the security and welfare of the person involved and any foreseeable outcomes to others
- Adequately consider and manage collateral intrusion
- Be proportionate (are lesser/alternative means that are less intrusive available?)
- Be cost-effective

6.4.15 In accordance with RIPA, authorities for directed surveillance are valid for up to 3-months from the date of the signature and up to 12-months for CHIS (1-month in the case of a minor under CHIS).

6.4.16 Further guidance on the application of RIPA including directed surveillance, CHIS and OSR is available from the Home Office/Office of Security Commissioners and the National Police Chiefs Council/College of Policing.