Meeting of Corporate Governance Committee on 19 March 2018
Item 9 – RIPA policy update
Information tabled by Officers at meeting to include in draft RIPA policy

1 Reason for this tabled note

- Since updating the above report, Officers have received guidance from the Investigatory Powers Commissioner's Office regarding the use of RIPA with regards reviewing and using information from social media sites.

- This note requests that Corporate Governance Committee agree for the below sections to be inserted into the draft RIPA Policy that it has before it today for approval.

2 Sections of the policy to update

- Officers request the following draft policy sections are updated.
- Page 2 of the policy (page 35 of the agenda) insert "Investigation of Social Media" as second item on page 62 of the policy (page 95 of the agenda).
- Page 6 of the policy (page 39 of the agenda) add a paragraph "Careful consideration should be given when using Social Media to obtain information as it may be subject to formal RIPA authorisation and approval, see page 62 of this policy for guidance".
- Page 34 of the policy (page 67 of the agenda) add a paragraph "Careful consideration should be given when using Social Media to obtain information as it may be subject to formal RIPA authorisation and approval, see page 62 of this policy for guidance".
- Page 62 of the policy (page 95 of the agenda) add a section as shown below:-

Investigation of social media

Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case *directed surveillance* authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example, a "friend" on the Facebook site, with the investigating officer utilising a false account concealing his or her identity as a Council officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at the minimum, as *directed surveillance*. If the investigator engages in any form of relationship with the account operator then that investigator becomes a *CHIS* requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created.