Derby City Council

COUNCIL
24 July 2019

ITEM 14

Report sponsor: Strategic Director of Corporate Resources:
Report author: Head of Legal Services

Appointments for Access to Communications Data

Summary

1.1 The Investigatory Powers Act 2018 ('the Act') came into force at the end of May 2019. It brings together under one legislative umbrella all of the investigative powers available to public bodies that undertake regulatory and/or criminal investigations where those activities involve the acquisition of communications data.

1.2 The Act also creates a new oversight body, the Investigatory Powers Commission (IPC), to oversee how the powers are used by each of those public bodies.

1.3 The Act requires each public body to nominate officers to act as a single point of contact (SPoC) between the body and the National Anti-Fraud Network (NAFN), who act as the gateway for all local authorities seeking to access permitted communications data from communications service providers. It also requires the appointment of a further officer to act as senior responsible officer (SRO), with oversight responsibilities over the integrity of the communications data access process within the council.

1.4 This report seeks a decision from Council to nominate two SPoCs for the purposes set out in the preceding paragraph.

Recommendations

2.1 To appoint the:

(a) Senior Corporate Fraud Officer; and
(b) Team Leader, Trading Standards

as Single Points Of Contact for the purposes of the Investigatory Powers Act 2018.

2.2 To appoint the Monitoring Officer as the council's Senior Responsible Officer.

2.3 To authorise the Monitoring Officer to make appropriate amendments to the Scheme of Delegations within the Council Constitution to reflect the appointments set out in recommendations 2.1 and 2.2.

Reasons for recommendation

3.1 To secure compliance with the provisions of the Act.

3.2 To ensure that the council has in place effective mechanisms to enable it access

communications data lawfully and legitimately when such a need arises in the performance of one or more of its enforcement activities.

3.3 To ensure that the constitution remains up to date and relevant.

Supporting information

4.1 The council has statutory responsibility for enforcement of a host of regulatory activity. The increasingly sophisticated methods employed by those flouting the law, notably a growing reliance on digital communication tools such as smartphone technology and the internet, necessitates enforcement authorities like the council having to adapt evidence gathering methods to suit. Consequently, it is becoming the norm to access communications data of those suspected of criminal activity.

4.2 In doing so however, there is a balance to be struck between public safety and the protection of personal freedoms. The Act's powers look to strike that balance by ensuring that access requests by public authorities are justifiable, necessary and proportionate. It does so by introducing a rigid application process that requires authorisation of applications by NAFN, who in turn liaise with one of the nominated SPoCs to test the integrity of every application prior to approval. If satisfied with the application, NAFN in turn routes the application through to another external body, the Office for Communications Data Authorisations (OCDA).

4.3 OCDA's role is to decide whether communications data access requests (i.e. applications) should be approved. It is described as a hub of authorisations expertise, holding authorities accountable against robust standards and challenging appropriateness of applications. OCDA has a target of 4-working days to approve, reject or return (for re-working) access requests. For this reason, the Act and NAFN guidance strongly suggest that the appropriate level of SPoC should be 'team leader' i.e. operational, so that where there is challenge, the SPoC should be able to respond to it at an operational level. This detracts from the council's established practice with other similar processes such as those in place under the Regulation of Investigatory Powers Act 2000 (RIPA), where its appointed authorising officers are all at service director level (i.e. the Director of Public Protection and Streetpride & the Service Director, Adults and Health).

4.4 SPoCs, once appointed, must have their details registered with NAFN. They are also required to access appropriate training and routinely refresh their acquired training knowledge to ensure their continuing appointment remains fit for purpose.

Public/stakeholder engagement

5.1 The requirement to appoint corporate SPoCs is a regulatory imperative and to that end, the need for public or stakeholder engagement as a prerequisite to doing so does not arise.

Other options

6.1 No other options have been considered as the Council has a statutory obligation to ensure that, in so far as any of its enforcement activities are likely to require access to permitted communications data, it has lawful arrangements in place for the purpose**.**

Financial and value for money issues

7.1 None arising from this report

Legal implications

8.1 As set out within the report.

Other significant implications

9.1 None arising from this report

This report has been approved by the following people:

Role	Name	Date of sign-off
Legal	N/A	
Finance	N/A	
Service Director(s)	Emily Feenan, Acting Director of Legal, Procurement and Democratic Services	12 July 2019
Report sponsor	Don McLure, Strategic Director of Corporate Resources	12 July 2019
Other(s)	N/A	

Background papers:	None
List of appendices:	None