Justice Sub-Committee on Policing

Police Scotland’s digital, data and ICT strategy

Data sharing

Further to your correspondence dated the 14th June (addressed to my colleague ACC Alan Speirs) I can provide the following information in response.

Police Scotland subscribe to a common Community Security Policy (CSP), which enables the cross-border exchange of data, including intelligence. Subscribers to the CSP include, not just the Home Office forces, but Scotland, PSNI, and many other Policing bodies. The CSP is underpinned by forces’ adherence to the Governance and Information Risk Return (the GIRR - formerly the National Policing Community Code of Connection) and is regulated under the governance of the Police Information Assurance Board, which has representation at SIRO (Senior Information Risk Owner) level from across Policing (not just Home Office forces).

UK Police forces have never operated information sharing agreements between themselves or in sharing data on national Policing systems. While information sharing agreements are a vital part of the relationship between Policing and other partners such as local authorities, we have long operated policing itself as a single community.

The exchange of information between law enforcement agencies and intelligence services will only be carried out if it is likely that it will be of value in:

- The interests of national security;
- The prevention or detection of crime and disorder;
- The maintenance of community safety;
- The assessment or collection of any tax or duty or of any imposition of a similar nature;
- Otherwise serves a significant public interest.

Police Scotland’s intelligence is routinely shared with the wider police service and a number of other law enforcement agencies via direct communication and also via the Police National Database (PND).

Police Scotland and the Metropolitan Police have directly shared information that may be recorded on the Metropolitan Police’s Matrix ICT system. In general terms, this information has related to intelligence about persons involved in the supply of controlled drugs and/or violence.

The PND is a national information and intelligence sharing system. It has been developed in response to the first recommendation of the Bichard Inquiry into the Soham murders.

The PND enables the police service and a number of other law enforcement agencies to share, access and search locally-held information on a national basis,
overcoming artificial geographical and jurisdictional boundaries. Data uploaded to PND should not be migrated to another system without the provider’s permission.

Data contributed to the PND from Police Scotland is limited to three sources: namely the Scottish Intelligence Database (SID), the Criminal History System (CHS) and the Scottish Organised Crime Groups Mapping (SOCGM). In general terms, Police Scotland uploads criminal intelligence, criminal histories and associated nominal details.

The PND and organisations providing data to PND are compelled to have regard to a number of legal and other obligations when deciding what information is submitted and how it is subsequently managed. The primary document defining these obligations is PND Code of Practice presented to Parliament pursuant to Section 39A of the Police Act 1996 which defines the principles governing the use of PND and the data held on it.

The Code of Practice:

a) Promotes the lawful and consistent use of PND and the information obtained from it
b) Mandates that Chief Officers adopt practices for the use of PND and the information obtained from it in order that such information is used effectively for policing purposes
c) Ensures that the operation of PND complies with data protection and human rights legislation
d) Ensures that PND is not used in a way which is discriminatory or otherwise unfair to anyone based on their age, race, ethnicity, any faith or belief, gender, gender identity, sexual orientation or any disability

The Code of Practice further states that the data on PND and the use of it must comply with Data Protection and Human Rights legislation, and the common law duty of confidence.

Information that is placed on PND must be managed in compliance with the guidance issued under code of practice on the Management of Police Information (MoPI) and the National Police Chiefs’ Council (NPCC) Data Protection Manual of Guidance.

If I can be of any further assistance please do not hesitate to contact me.

Steve Johnson
Assistant Chief Constable
Specialist Crime and Intelligence
26 June 2018