



JOB DESCRIPTION QUESTIONNAIRE (J.D.Q.)

HMI CATEGORY CODE:

DIRECTORATE: Intelligence
AREA/DEPT: Force Intelligence Bureau (FIB Covert)

FAU:

SECTION: Covert Authorities Bureau

JOB TITLE: **COVERT OPERATIONS DATA AND COMPLIANCE ADVISOR (CODA)**

REPORTS TO: Sergeant Covert Authorities Bureau

CURRENT RANK/GRADE: **E**

DATE: Dec 2022

1. JOB PURPOSE: (Briefly state your job's overall objectives. To.....")

To ensure that Merseyside Police meets its statutory obligations under data protection, data usage legislation and review, retention and disposal procedures (RRD) in relation to information relating to all covert data including communications data as required and overseen by the IPCO – Investigatory Powers Commissioner's Office.

To promote and ensure strong data protection and governance within the Force relating to covert data / information whilst assisting with the development of new processes and procedures to ensure compliance, with an emphasis on the review, retention and disposal of covert data. The postholder will champion good information management and data protection compliance by raising the profile of data protection policies and processes, recognising, and celebrating examples of exemplary compliance and data management behaviour, as well as sharing good practice.

2. PRINCIPAL ACCOUNTABILITIES:

(Describe the important end results you are expected to achieve).

- a) Provide tailored, comprehensive, well-structured and detailed data protection advice and guidance to colleagues about their statutory obligations under data protection legislation and their covert data safeguarding responsibilities (RRD).
- b) Draft and review Memorandum of Understanding agreements and Letters of Mutual Understanding between Merseyside Police, Home Office forces and other partner agencies.

- c) Conduct data protection guidance and awareness sessions to staff across the Force who deal with information / data relating to covert data.
- d) Support Information Asset Owners [IAOs] by providing advice and information.
- e) Assist with Data Protection Impact Assessments [DPIAs] and establish and maintain stakeholder relationships with the Data Sharing and Protocols Team.
- f) Identify and manage risks and promote and embed good information management behaviours and practices across the business by reference to the Information Risk Management Policy and related policies and procedures thereby maintaining the Information Risk Management Register.
- g) Liaise with Policy colleagues to provide operational assistance and support with future data protection / data sharing agreements.
- h) Lead on Data Safeguards in relation to material obtained through use of covert powers including assessing compliance with the relevant sections of the Codes of Practice that accompany IPA 2016 and RIPA 2000
- i) Review existing information sharing agreements, to ensure that they are still valid and fit for purpose and assist with the creation and monitoring of files associated with information sharing agreements.
- j) Ensure that Merseyside Police have appropriate internal policies for all aspects of data assurance relating to covert information / data including covert data pathways and that have appropriate governance and are kept updated.
- k) Undertake an ongoing programme of audits to ensure that covert data / information held comply with the UKGDPR and DPA, ensuring the organisation achieves and maintains compliance and that processing of personal data, and other information in electronic systems and other manual processes complies with relevant legislation by ensuring that security arrangements are in place to protect information, including where necessary, contracts relating to third parties processing information.
- l) Must maintain a recording system appropriate to the efficient operation of the audit programme allowing management and performance information to be produced.

- m) Be accountable for all Health and Safety issues, including risk assessment, pertaining to the post holder's area of responsibility in order to fulfil the statutory obligations of the Health and Safety at Work Act 1974
- n) Undertake all responsibilities relating to information management, data quality and information sharing, intelligence and information security and the Review, Retention and Disposal of covert data to ensure accordance with the Authorised Professional Practice (APP) on Information Management, issued by the College of Policing

3(a) KNOWLEDGE AND EXPERIENCE:

(What kind of knowledge, skills and experience are necessary to enable satisfactory performance in the job and why are they necessary?).

Educated to Degree / Level 6 of the Qualifications & Credit Framework (QCF) equivalent in a relevant subject and / or significant experience of working in a information management / data protection role.

Display strong organisational and planning skills, with good attention to detail.

Ability to work effectively and professionally with minimal supervision in a highly pressured environment.

Building, developing, and maintaining strong and effective working relationships at all levels, internally and externally, through collaboration and professional credibility.

Experience and ability to build a strong network and promote collaborative working that reaches appropriate compromises when necessary to achieve the best outcome.

An ability to work independently as well as being an excellent team player.

Be comfortable working with ambiguity, weighing up options in complex data protection and data sharing scenarios and making effective recommendations and decisions based on sound judgement

Acting as an excellent communicator and a strong influencer who can provide constructive challenge at all levels.

Demonstrating a strategic and operational mind-set with the ability to execute excellent judgement.

The post holder must have a detailed knowledge of the appropriate national standards and legislative requirements for Information Assurance, United Kingdom General Data Protection Regulations (UKGDPR) and Data Protection Act 2018 (DPA) and their application.

Understanding of the role of the IPCO – Investigatory Powers Commissioner’s Office.

Sound negotiation and influencing skills are essential, to enable the post holder to complete information management activity across the force, supporting the Data Protection Officer and Information Security Officer as well as the Information Asset Owners, in their responsibilities.

Report writing and presentation skills are essential to strategically position the Information Asset Owners and key members of the Force on all matters relating to data protection and information assurance. In addition, the post holder will be required to produce policies, procedures and guidance on data protection and information assurance matters that reflect strategic and operational requirements.

3(b) (Does your post require any Police Powers, and if so what are they, and why are they necessary?)

N/A

4. RELATIONSHIPS:

(a) *Supervisory responsibilities:*

N/A

(b) *Supervision Received:*

The post holder will report directly to the Sergeant Covert Authorities Bureau but will have direct contact with Force Authorising Officer (D/Supt)

The post holder will be expected to use their own initiative and work with minimum supervision.

(c) *Other Contacts:*

(i) *Within Merseyside Police:*

Daily contact with all functional policing areas through the Force including SIO’s to major investigations.

Regular contact with Data Protection Officer and Information Security Officer

Regular contact with Force Information Asset Owners, supporting them throughout the audit and risk management process, including the implementation of agreed action plans, tracking and monitoring action through to completion.

(ii) *Outside Merseyside Police:*

Regular contact with NWROCU as Merseyside is the lead force with regards to the Covert Authorities Bureau (CAB). Contact with other forces and partner agencies including the Crown Prosecution Service and National Crime Agency.

As and when contact with IPCO – Investigatory Powers Commissioner’s Office

5. CONTEXT:

(a) *Operating Environment:* (Services provided, work patterns, who are the customers).

The post holder will be required to work within the Force Flexible Working Hours Scheme, Monday to Friday. The post holder needs to be flexible to meet any exceptional demands placed on the Force or the department. The post holder may be required to travel for business purposes.

(b) *Framework and Boundaries:* (Policies and procedures which affect you and how these can be changed).

Intrusive Surveillance is governed by Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016, Human Rights Act 1998 and Part III of Police Act 1997. Interrogation of the Force Intelligence System and a working knowledge the United Kingdom General Data Protection Regulations (UKGDPR) and Data Protection Act 2018 (DPA), Misuse of Computer Act and CPIA.

(c) *Organisation:* (For each type of post that reports directly to you, outline below the posts overall responsibilities).

N/A

6. DIMENSIONS: (Indicate in quantitative terms, key areas on which your job has an impact).

Financial: N/A

Staff: N/A

Other: Adopting sound information processes, policies and procedures will enable the Force to put into place effective measures to prevent unauthorised access to or loss/destruction of information. This not only demonstrates integrity around information handling but could potentially avoid the costs and implications of major investigation and adverse publicity, thereby protecting the reputation of the Force whilst achieving an enhanced degree of compliance with the legislation

7. JOB CHALLENGES: (Describe the most challenging or complex parts of your job).

It is essential that the Force complies with the DPA, UKGDPR and other related legislative requirements, statutory Codes of Practice and other national requirements in the way in which we record, retain, use and delete our information. This requires the Force to optimise the knowledge of all Force employees, contractors and partner agencies around data protection and information assurance matters.

There is a need to balance the demands of keeping our covert information / data secure and making sure our information is accessible to partner agencies. The increasing requirement for sharing data and information with our key partner agencies needs to be overseen to reduce any risks to the security of information held by the Force.

The postholder will undertake continuous personal and professional development and take personal responsibility for keeping up to date with changes in relevant information legislation and best practice.

8. ADDITIONAL INFORMATION:

(Provide any further information, not included in your previous answers, which you consider would assist others to achieve a better understanding of your job).

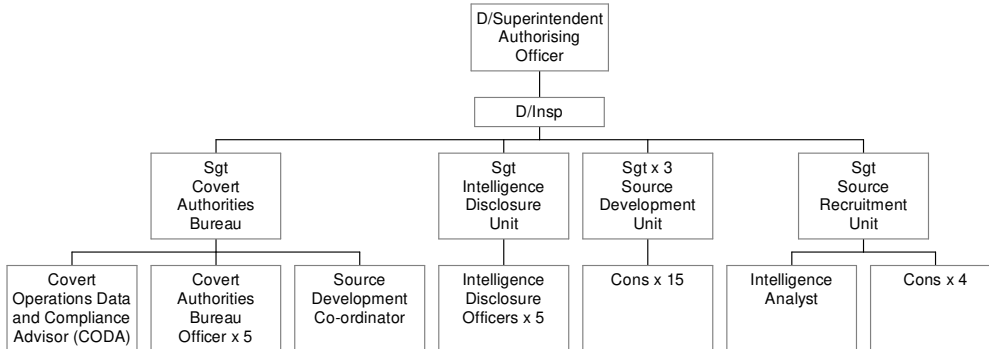
This post will be subject to vetting checks to MV and SC level prior to taking up the post.

While post holder does not have any supervisory role within own right, by virtue of position post holder has a responsibility for ensuring compliance with safeguarding / RRD policies.

The post holder must have a high level of initiative and a flexible and innovative approach with sound leadership, decision making and problem-solving skills.

9. ORGANISATIONAL STRUCTURE:

(Draw an organisational chart of your Department / Section, indicating the position of your post within it).



10. AGREEMENT OF QUESTIONNAIRE CONTENT:

(Please sign when completed)

POSTHOLDER'S NAME:

(Please print in block capitals)

POSTHOLDER'S SIGNATURE:

Date:

Extn

MANAGER'S NAME:

(Please print in block capitals)

MANAGER'S SIGNATURE:

Date:

Extn