JOB DESCRIPTION QUESTIONNAIRE (J.D.Q.)

HMI CATEGORY CODE:
DIRECTORATE: Intelligence
AREA/DEPT: Force Intelligence Bureau
FAU:
SECTION: Digital Media Intelligence Unit (DMIU)
JOB TITLE: **DIGITAL MEDIA INTELLIGENCE OFFICER (POLICE STAFF)**
REPORTS TO: Sergeant (DMC) Digital Media Intelligence
CURRENT RANK/GRADE: **D**
DATE: July 2017

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

To utilise specialist skills and techniques to research, exploit and capture information available from on-line sources (open & hard to reach 'dark web'), in order to obtain intelligence to address the Threat, Risk and Harm affecting the communities of Merseyside.

To actively contribute to the coordination of 'open source' operating procedures, policy and best practice, acting as a central point of expertise to 'Digital Media Investigators' across the organisation.

2. PRINCIPAL ACCOUNTABILITIES:

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

a) As a trained Digital Media Investigator (DMI), use specialist techniques to strategically plan Force level 'Open Source' responses, with a view to contributing to intelligence development packages, serious crime investigations and major event planning prioritising intelligence collation around threat, harm and risk.

b) Develop intelligence from 'online' information for operational purposes. Grade, input, evaluate and appropriately disseminate, actionable intelligence at the earliest opportunity, to support the Force strategic and tactical assessments.

c) Prepare and deliver timely and accurate intelligence products in order to direct and focus Police resources at tactical and strategic level. Prepare operational plans and on occasion, conduct quick time research in response to developing incidents and crimes in action, in order to provide the most accurate intelligence picture to supervising officers.

d) Provide strategic and tactical advice to Chief Officers, Business Strand Leads, Operational Commanders and Senior Investigating Officers including reports about techniques and opportunities to exploit open source information, the handling of such information in accordance with the law and the production of products, documents and the presentation of information to a range of audiences.

e) Assist the Digital Media Coordinator with disseminating best practice and guidance to the network of Digital Media Investigators and Mainstream Cyber trained staff across Merseyside Police, to achieve a comprehensive force-wide response to both cyber-enabled and cyber-dependent crimes as well as wider criminal activity.

f) Coordinate 'Digital Media Intelligence' policy and operating procedures across Merseyside Police, acting as a central point of expertise for the organisation. Be responsible for implementing new procedures and techniques across the Force, providing advice and guidance to DMI's and other trained staff.

g) Conduct 'online' horizon scanning, to identify new platform and applications (apps) used by the general public that may provide potential intelligence opportunities. Following research and testing, identify techniques and procedures to best exploit applications to enhance and improve intelligence gathering and development.

h) Provide a point of expertise within Merseyside Police to develop partnerships with external agencies (law enforcement, NCA, local authorities, government departments) in order to progress 'digital' intelligence development and serious crime investigations into offences involving both traditional and cyber-crime types.

i) Provide advice and guidance to officers and staff throughout the Force to ensure internet safety, compliance with legislation and correct methodology are applied.

j) Undertake all responsibilities relating to information management, data quality, information sharing, intelligence and information security to ensure accordance with the Authorised Professional Practice (APP) on Information Management, issued by the College of Policing including Home Office Code of Practice on MoPI.

k) Be accountable for all Health and Safety issues, to include risk assessment, pertaining to the postholder's area of responsibility in order to fulfil the statutory obligations of the Health and Safety at Work Act 1974.

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?).

Hold accreditation as a Digital Media Investigator (DMI) or be prepared to attain such accreditation.

Previous experience of working in Operational Intelligence would be desirable.

Postholder should be computer literate, be able to develop skills in line with advances in digital media and ability to undertake in depth research on the internet.

Good knowledge of current Threat, Risk & Harm, Force priorities and current Force investigations to provide advice and support to other DMI's/operational officers around the Force in relation to Cyber Crime.

To have proven communication skills confidence to provide specialist advice and liaise at all levels, both internally and externally.

To have a high level of self-motivation and be able to work under pressure, with a flexible approach to changing circumstances to undertake the role effectively.

Excellent working knowledge of RIPA and CPIA, experience of making applications for Communications Data / Directed Surveillance would be desirable.

Excellent understanding of OSC (Office of Surveillance Commisioners) Procedures and Guidance.

3(b)

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

In urgent circumstances this role may form part of an intelligence cell and may be deployed anywhere to support intelligence gathering, obtained warrants or undertake operation duties.

4. RELATIONSHIPS:

(a) Supervisory responsibilities:

No supervisory responsibly, however the post holder will drive best practice to DMI's within other business strands, in order to develop good practice and ensure legislative compliance.

(b) Supervision Received:

Daily contact with the DMIU Sergeant

(c) Other Contacts:

(i) Within Merseyside Police:

Contact across the Intelligence Department, with area based DMI's and mainstream cyber trained staff.

Responsible for briefing operational staff including Chief Officers.

(ii) Outside Merseyside Police:

Regular contact with forces with partners from other law enforcement and government agencies, computer application providers, Communication service providers.

5. CONTEXT:

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

The post holder should have a flexible approach to working hours to meet demand. Post holder works within the Force Flexitime Scheme.

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

All Merseyside Police policies are applicable to the role.
The Data Protection Act 1998
Criminal Procedure and Investigation Act
Police and Criminal Evidence Act 1984
Management of Police Information
The post holder will need to remain up do date with current case law, procedural rulings and developments across the field. Compliance with Health & Safety and Human Rights legislation is required and with the Force
Diversity policies.

***(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: Nil

Other: N/A

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

This is a developing and demanding role requiring a methodical, well-organised and thorough approach.

The timely and accurate dissemination of time critical intelligence.

8. ADDITIONAL INFORMATION:

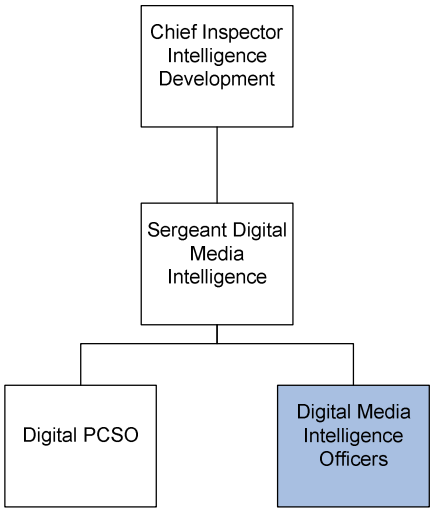
(Provide any further information, not included in your previous answers, which you consider would assist others to achieve a better understanding of your job).

The post holder will be required to undertake an entry assessment and be subjected to vetting checks to MV

Postholder should lead by example, take responsibility for own development attaining accreditation of IPP, behaving in line with the Code of Ethics and Force Purpose and Values

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: