



## ROLE PROFILE

<b>Role Title</b>	Head of Digital Forensic Unit	<b>Reporting to</b>	Detective Superintendent
<b>Section</b>	Digital Forensics Unit	<b>District/Department</b>	Protective Services Crime
<b>Tenure</b>		<b>Rank/Grade</b>	POF

### Part A – JOB DESCRIPTION

<b>Overall purpose of role</b>	To provide overall management to the Force DFU, Cyber and DMI capabilities and strategic direction to the Force on the development and application of Forensic Digital techniques, ensuring the provision of an effective, efficient and comprehensive Digital Forensics Service to the Force. Promote innovation and development through the continuous improvement of systems, processes, working practices and technology.
--------------------------------	---

<b>Key outputs for role –</b>	
<ol style="list-style-type: none"><li>1. Lead by example and behave in line with the Police Code of Ethics ensuring that the force values and behavioural expectations are clearly understood and considered by managers, officers and staff in their decision making and actions; reinforcing and influencing them through all interactions and processes.</li><li>2. Responsible for the strategic development of the vision and objectives for Force Digital Forensics, ensuring strategic alignment with Force and PSC objectives and priorities. In addition, take responsibility for ensuring the strategic response, formulation and implementation of policy, procedures and guidelines for all aspects of work to satisfy Force, Forensic Science Regulator Codes 17025 and ISO 17020 requirements in order to comply with relevant legislation.</li><li>3. Proactively manage the performance, attendance and wellbeing of police officers and police staff against the required standards to ensure they are dealt with and supported in accordance with the correct policies and procedures.</li><li>4. Responsible for the overall strategic operational and performance management of staff within the Digital Forensics Unit (DFU), making the most effective and efficient use of resources to meet demand and optimise service delivery and resilience.</li><li>5. Lead, manage and coordinate the overall tactical delivery of digital forensic services across the force. Provide the role as Force SPOC in relation to relevant developments in Digital Forensic Investigations advising Chief Officer Team and other SLT members, making recommendations that will lead to continuous improvement in the quality of investigations, and provide direction and delivery in relation to the Force Policies and Procedures.</li><li>6. Ensure that management information is developed, compiled and assessed in relation to the performance and productivity of all elements of Digital Forensic Investigations and ensure appropriate progress is made against Service Level Agreements.</li><li>7. Identify and promote best practice across the Force, Region and nationally, ensuring WYP are represented and at the forefront of future developments to processes, systems and technology in respect of Digital Forensics. Working with partners and representing the Force at a regional and national level, (e.g. Transforming Forensics, NETIC).</li><li>8. Ensure the completion of audit &amp; inspection processes and the investigation &amp; resolution of complaints. Identifying quality of service issues including any inefficient equipment, practices or procedures, identifying potential improvements, to maintain and improve quality of service.</li></ol>	

**Dimensions** (Financial/Statistical/Mandates/Constraints/No. of direct reports)

- Management of Operational and Investigation budgets to the value in excess of £2m.
- Management responsibility for up to 3 staff directly, with overall management of at least 150 staff.
- Investigations must be conducted in full compliance with Force Policy, ACPO Guidance, PACE, CPIA, RIPA and ECHR legislation.
- The proactive identification and implementation of improvements to processes, systems and the driver to forward thinking working practices within the DFU.

**Work/Business contacts**

**Internal:** Chief Officer Team, SIO's, HMET staff, District Chief Superintendents, Crime Managers, District Safeguarding Leads, NPT Supervisors, Crime Scene Examiners, SSU, Protective Services Crime Specialist Units.

**External:** Regional Cyber Unit, CPS and appointed Counsel, other Forces, National Crime Agency, College of Policing, Home Office, Outsourcing companies.

**Expertise in Role Required (At selection - Level 1)****Essential or Desirable**

- |  |           |
|--|-----------|
| • Demonstrate strategic understanding and management experience at a senior level of a digital forensic environment      | Essential |
| • Knowledge and experience of ISO 17025, 17020 accreditation and Forensic Science Regulator Codes.                       | Essential |
| • Ability to prioritise workload to deliver service provision to meet customer requirements and Service Level Agreements | Essential |
| • Has a good knowledge and understanding of Computer Systems.  | Essential |
| • Experience of working in partnership at a strategic level.   | Essential |
| • Ability to adapt to and environmentally scan for new technological advancements.                                       | Essential |
| • Experience of serious crime management and investigation   | Desirable |
| • Has a detailed knowledge of Criminal Law and Court processes.  | Desirable |
| • Has an understanding of crime scene interpretation and potential forensic opportunities.                               | Desirable |
| • Understanding of the MAPPA process and Sex Offender Legislation  | Desirable |

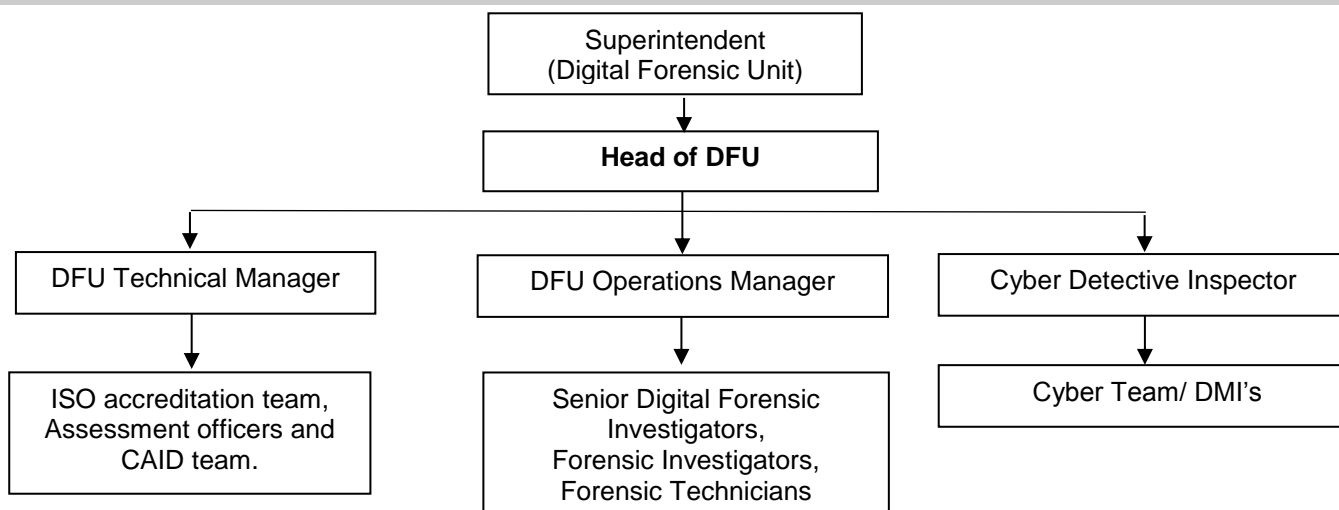
**Other (Physical, mobility, local conditions)**

- |  |           |
|--|-----------|
| • Be prepared to follow an on-call arrangement for immediate response if required.   | Essential |
| • Prepared to successfully undertake management vetting, including financial checks  | Essential |
| • Prepared to work flexibly to meet the needs of the department  | Essential |
| • Although a 'Normal place of duty' will be identified, work could be undertaken at any of the Force locations   | Essential |
| • Due to the nature of the work and investigations carried out within the DFU it is highly likely the post holder will be exposed to material of an abusive and offensive nature, including graphic child abuse imagery. | Essential |

### **Expertise in Role - After initial development - Level 2**

- Achieved and demonstrated a detailed knowledge of ISO 17025, 17020 Accreditation and Forensic Science Regulator Codes.
- Achieved and demonstrated a detailed knowledge of police structures, policies and procedures across the Force relating to personnel issues, e.g. attendance management and health and safety
- Utilises contacts, partnerships and communication skills to the benefit of Digital Forensics and enhancing Force capability.
- Achieved a greater understanding of crime scene interpretation and forensic opportunities.
- Detailed knowledge of relevant legislation and processes.
- Knowledge of current and future CAID (Child Abuse Images Database) operating requirements.
- Demonstrates an ability to drive change and review performance of the department
- Demonstrates an ability to deliver innovative technology in the Digital Forensic field.

### **Structure**



## **PART B – COMPETENCIES & VALUES**

### **Competency and Values Framework –**

[http://www.college.police.uk/What-we-do/Development/competency-and-values-framework/Documents/Competency-and-Values-Framework-for-Policing\\_4.11.16.pdf](http://www.college.police.uk/What-we-do/Development/competency-and-values-framework/Documents/Competency-and-Values-Framework-for-Policing_4.11.16.pdf)

### **Select one level**

Level 3 – Senior Manager/Executive

## **PART C - DEVELOPMENT OF ROLE**

### **Expertise in Role (Advanced - Level 3)**

- Is recognised as an expert source of advice relating to Digital Forensics
- Has undertaken project development work at a national level to advance digital forensics.
- Developed a comprehensive network of internal and external professional contacts

- Recognises and develops best practice in the investigation of child sexual exploitation and other relevant crimes and disseminates this throughout Protective Services Crime, Districts and other Force Departments.
- Has delivered improvements to working practices, process and systems through the identification and integration of innovative technology and best practice from other Forces and relevant Organisations.
- Has developed effective working relationships with leading Academics to ensure continued innovation through transformational change opportunities.

## **PART D - ACCESS & VETTING**

<b><i>Standard IT Access</i></b>	Default
<b><i>Police Building (Perimeter and Zone access)</i></b>	Perimeter Access to buildings where based
<b><i>Vetting Level</i></b>	Management vetting and Security Clearance
<b><i>Date accepted as a role profile</i></b>	16.12.2019