# ROLE PROFILE

| | | | |
|---|---|---|---|
| **Role Title** | CT Digital Investigations Manager | **Reporting to** | Head of Forensic and Digital Investigations / Quality Manager - Principal Forensic Evidence and Exhibits (FEE) Officer |
| **Section** | CT Digital Investigations | **District/Department** | CTPNE |
| **Tenure** | | **Rank/Grade** | POB |

## Part A – JOB DESCRIPTION

| **Overall purpose of role** | Undertake the day to day management of the CT Digital Investigations Team, providing technical knowledge and investigative skills in all aspects of CT digital investigative functions. Ensure the provision of an effective, efficient and comprehensive CT Digital Forensics Service in support of regional, national and international Counter Terrorism Policing, whilst promoting innovation and development through the continuous improvement of systems, processes, working practices and technology. |
|---|---|
| | Working in conjunction with the Quality Manager and undertake the Technical Manager role within CT Digital Investigations scope of accreditation, providing specialist technical expertise, skills and knowledge in Digital Forensics relevant to the implementation and maintenance of ISO17025/17020 accreditation and other associated legal and regulatory standards, ensuring that the department remains and operates in full compliance. |

**Key outputs for role –**

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.

2. Proactively manage the performance, attendance and wellbeing of police staff against the required standards to ensure they are dealt with and supported in accordance with the correct policies and procedures. Set and manage training plans for staff, maintaining records.

3. Responsible for managing the workload, performance management and productivity of staff within the CT Digital Investigations department. Make effective use of CT resources to provide the highest level of service delivery to meet demands and optimise service delivery. Provide staff with clear direction to enable them to effectively and efficiently meet the requirements and demands of the department and ensure a consistent approach to the acquisition, processing, analysis and investigation of digital devices, which may have been used in the terrorism offences and associated criminal offences, in line with ISO and NPCC guidance.

4. Responsible for ensuring that all digital examinations and investigations are assessed, prioritised, interrogated and analysed in line with CT SIO requirements, making risk based decisions whilst taking into account the potential level of threat, risk and harm, relevant legislation and technical complexity associated with each case, taking responsibility for those decisions. Provide expert technical advice and produce case specific strategies where necessary. Be responsible for monitoring and conducting peer-reviews of work and technical evidential reports produced by staff to ensure that the Forensic Regulator Codes and ISO 17025 standards are maintained and adhered to.

5. Lead the development of Technical procedures within CT Digital Investigations department, maintaining an awareness of current research and development in relation to Digital Forensics, ensuring that processes and procedures are completed to consistently high standards in accordance with all UKAS/ISO/FSR requirements, maintaining a comprehensive manual to support staff and ensure consistency and compliance.

6. Manage an extensive workload and participate in the provision of a digital investigation response from initial operational briefing to scene attendance, investigative work and presentation of evidence in court for cases related

to terrorism offences, hostile state actor, serious and organised crime and other associated criminal offences. Using expert knowledge, provide appropriate advice and guidance to investigators and SIOs to ensure that investigations are focussed and maximise forensic investigative opportunities, ensuring agreed investigation timeframes are met.

7. Work in conjunction with the Quality Manager to conduct scheduled internal and technical audits, competency assessments and quality assurance testing, such as dip sampling, to identify non-conformances and opportunities to improve the quality of service. Provide technical assistance in quality management investigations resulting from audits, issues and complaints. Advise on immediate containment actions, agree corrective and preventive solutions and implement effective findings in a timely manner. Identify quality of service issues including inefficient equipment, practices or procedures, identifying potential improvements and solutions to maintain and improve quality of service. Prepare summary information/reports for management to demonstrate compliance with FSR/ISO requirements. Oversee all validation and software update procedures as required.

8. Oversee the management of the Digital Investigations Network and Server through the use of appropriate support and maintenance, access control, security, updates, RRD and upgrades and other server administrative tasks to support the efficient function of the CT Digital Forensics Network, working closely with equipment suppliers and mutual support agencies to ensure and maintain awareness of technology, legislation and techniques.

9. Utilising extensive technical expertise and experience to routinely contribute to and implement numerous national/international digital innovation projects to help mitigate ever evolving complex counter terrorism, hostile state actor and serious and organised crime digital threats.

---

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

- Management responsibility for CT Digital Investigators involvement in a high quality professional service in the retrieval, investigation, interrogation and analysis of digital evidence from 1000's of digital exhibits per year seized from a variety of terrorist related incidents/investigations, HAS, SOC and other associated criminal offences.

- Second line management responsibility for CT Digital Media Assessment Team in the provision of a high quality comprehensive Digital Media Assessment service of vast quantities of digital artefacts.

- Up to 12 direct reports and a team of up to 20.

- Support Head of FDIT and Quality Manager in ensuring the CT Digital Investigations Department are compliant with force policies, Forensic Science Regulator Codes and ISO 17025/17020.

- The ongoing identification and implementation of improvements to processes, systems, working practices and value for money within CT Digital Investigations.

- Working regionally, nationally and possibly internationally if required for potentially prolonged periods.

---

### *Work/Business contacts*

**Internal:** SIO's, Senior Leadership, Forensic Management Team, OIC's, Investigations and Intelligence Teams, Digital Investigations Staff, Digital Media Assessment Team, Partner Agencies, Ports, Prevent, Prisons and other CT teams from all ranks including Image Recovery & Analysis team, Ports, Prevent and Prisons.

**External:** Work in partnership with other NDES, CTPs, CTIUs, SBs and Regional/National Forces, domestically and internationally. External agencies such as CPS, UK and International Intelligence Services, defence experts, external suppliers and hardware/software vendors.

---

| *Expertise in Role Required (At selection - Level 1)* | Essential or Desirable |
|---|---|
| - Degree in Computer Science/Forensic Computing Studies or equivalent qualification in Digital Forensics and/or significant proven experience/training in these fields. | Essential |
| - | |
| - Advanced knowledge and expertise of common operating systems, applications, basic network technologies and internet technologies. | Essential |
| - Advanced understanding of the Forensic analysis of digital devices with experience of working on a variety of crime types, including serious and complex cases, preparation of evidence and court testimony. | Essential |

| | |
|---|---|
| • Ability to prioritise and manage workloads, work under pressure and make critical decisions to deliver service provision in order to meet customer requirements and Service Level Agreements | Essential |
| • Ability to attend and pass requisite Digital Forensics training courses and achieve and maintain accreditations where applicable. | Essential |
| • Recognising and handling sensitive information, maintaining the utmost discretion and confidentiality at all times. | Essential |
| • Willingness to attend live scenes and terrorism related incidents to provide expert digital forensic coordination to first responders, investigating officers, SIO's and partner agencies. | Essential |
| • Knowledge and experience of ISO17025 accreditation and Forensic Science Regulator Codes. | Desirable |
| • Willingness and ability to undertake CBRN training and associated activities, including the performance of digital coordination activities in unpleasant and contaminated scene environments and potential Warm zone areas. Including attendance on National and International CT / Military / CBRN exercises providing a specialist Digital Forensics coordination service. | Desirable |
| • Previous supervisory/management experience. | Desirable |
| • Knowledge, experience and understanding of Counter Terrorism / Operational Policing. | Desirable |
| *Other (Physical, mobility, local conditions)* | |
| • Ability to conduct visual, peer review and other quality control mechanisms | Essential |
| • Physical and emotional resilience to deal with offensive and abusive images of extreme violence, obscenity and depravity. | Essential |
| • Willingness to undergo Psychological Assessments, as and when required | Essential |
| • Willingness and ability to travel for business purposes, regionally, nationally & internationally for business purposes possibly for extended periods and at short notice | Essential |
| • Willingness and ability to work unsociable hours, 24 hour cover, to change hours at short notice and participate in call-out rota if required | Essential |
| • Full UK/European Driving Licence | Essential |
| • Access to a vehicle for Business purposes | Desirable |
| • Willingness and ability to successfully undergo MV / SC / DV vetting procedures | Essential |

---

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

- Experience in managing complex digital investigation cases relating to terrorism offences, including development of digital strategy, prioritisation of workload and peer review of staff work.

- Advanced knowledge of a variety of digital forensic hardware and software tools relevant to the role

- Successfully completed the recommended training courses

- Has developed working knowledge of relevant criminal law, policies and procedures relevant to the role e.g. CPIA, PACE, RIPA, Human Rights Act, GDPR, Terrorism Acts and legislations

- Successfully deemed competent in all digital forensic processes in line with the requirements of the Quality Manual

- Ability to undertake CBRN training and CBRN activities, including the coordination of digital activities in unpleasant and contaminated environments

- Has overseen/conducted scheduled technical audits, identified non-conformances and provided technical assistance in quality investigations resulting from audits, issues and complaints.

- Has delivered improvements to working practices/technical procedures, processes and systems through the identification and integration of innovative technology and best practice in partnership with internal and external organisations

- Ability to plan and conduct quality assurance testing in addition to assessing, developing and managing validation procedures for new techniques for accreditation

- Advanced knowledge of network administration, server management and effective data backup technologies and procedures

| Structure |
| --- |
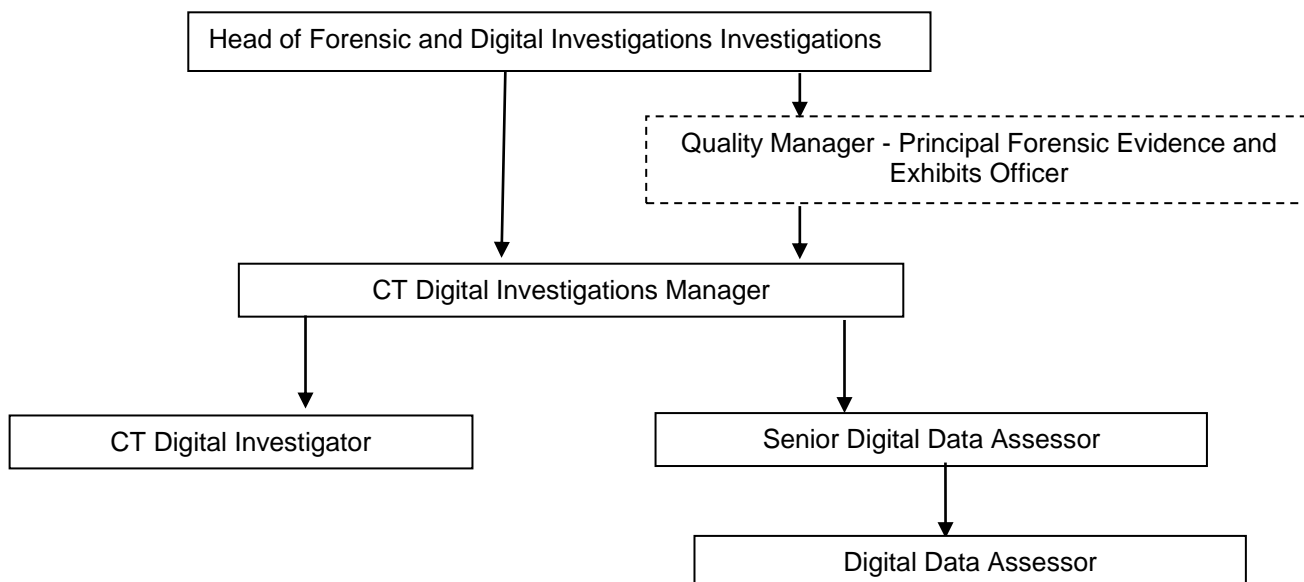


## PART B – COMPETENCIES & VALUES

| ***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 |
| --- |
| Level 2- Supervisor/Middle Manager |

## PART C - DEVELOPMENT OF ROLE

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

- Recognised as an expert in this field

- Developed a comprehensive network of internal and external professional contacts

- Play a key role in obtaining / maintaining Digital Investigation accreditations or standards

- Recognises, develops and delivers improvements to working practices, processes and systems through the identification and integration of innovative technology and best practice from CT network, CT wider community and other relevant organisations

- Routine contribution to national / international digital capability innovation projects

## PART D - ACCESS & VETTING

| | |
| --- | --- |
| ***Standard IT Access*** | Default |
| ***Police Building (Perimeter and Zone access)*** | Perimeter Access to buildings where based |
| ***Vetting Level*** | DV |
| ***Date accepted as a role profile*** | 17th December 2020 |