WEST YORKSHIRE POLICE

ROLE PROFILE

Role Title	Counter Terrorism Digital Forensic Investigator	***Reporting to***	Senior Counter Terrorism Digital Forensic Investigator
Section	Digital Investigations	***District/Department***	CTP NE
Tenure		***Rank/Grade***	

Part A – JOB DESCRIPTION

Overall purpose of role	To conduct digital forensic investigations of all digital devices to obtain evidence and intelligence in support of regional, national and international Counter Terrorism Policing.

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. Provide specialist technical input and guidance to law enforcement officers, routinely accompanying them to conduct overt and covert captures of digital evidence/intelligence. Also responsible for the provision of expert consultative services at both Pre and Post executive phase briefings.
3. Responsible for the continuity of all digital exhibits maintaining their integrity during a digital forensic investigation. Conduct the forensic acquisition, analysis and investigation of evidence/intelligence from a variety of digital sources which may have been used in the commission, preparation or instigation of acts of terrorism and associated serious criminal offences.. Data retrieved may contain highly confidential and potentially indecent, extreme or offensive information which must be retrieved in a forensically sound manner with its integrity maintained for subsequent submission to Court.
4. Produce court packages including; evidential material of the highest standard; written statements, expert detailed forensic reports and the Electronic Presentation of Evidence (EPE). Attend court both nationally and internationally as a subject matter specialist witness. Represent CTP NE at CPS Case Conferences, liaising with Prosecution/Defence Barristers, Defence Experts and the Judiciary.
5. Ensure compliance with the CTP NE Quality Manual, working to obtain and maintain ISO17025 and ISO17020 accreditation in line with the Forensic Science Regulators requirements and Codes of Conduct. Guarantee accurate recording of examination records following unit standard operating procedures whilst supporting the documentation of methods for extension to scope. Participate in quality audits, competency checks, peer reviews and exhibit re-tests, identifying and reporting non-conformities to the Quality Manager.
6. Provide expert advice and guidance to personnel within the National Counter Terrorism Network, liaising with staff of all ranks, including SIO's, Intelligence Services and NDES, to ensure that all digital opportunities are explored, sourced and maximised for the timely production of evidence/intelligence in accordance with national guidelines, SIO's Digital Strategy and authorisation levels.
7. Understand, implement and actively promote Digital Forensics best practice methodologies in line with the NPCC Guidelines for Digital Evidence in the retrieval, handling and examination of digital based exhibits. Maintain awareness of criminal law and procedures relevant to the role working within TACT, GDPR, RIPA, FOIA, CPIA, PACE and other relevant legislation ensuring compliance at regional, national and international levels.
8. Assist in the development and delivery of bespoke training packages, lectures and demonstrations to both technical and non-technical persons, including Police Officers, Police Staff and other agencies offering awareness and advice as required.
9. Participate in the construction, rollout and maintenance of dedicated Digital Investigation computer, mobile phone equipment and software. When required, maintain the Digital Investigations Network and server through the use of appropriate support and maintenance, access control, security, updates and upgrades and other administrative tasks to support the efficient functioning of the network.

Dimensions *(Financial/Statistical/Mandates/Constraints/No. of direct reports)*
• Working within relevant accreditation standards following the Units Quality Manual and Forensic Science Regulators Codes of Conduct. • Responsible for the mentoring and training of new staff. • May produce 2+ complex EPEs (Electronic Presentations of Evidence) per year An EPE could take over 200 working hours to produce. • Provide complex and detailed Forensic Reports and statements for SIOs / Investigating Case Officers and CPS. Approximately 6+ per year. A detailed forensic report could take 100+ working hours to produce.

Work/Business contacts
Internal: SIOs, Senior Leadership, Forensic Management Team, OIC's, Investigations and Intelligence teams, Digital Investigations Staff, Digital Media Review Team, Partner Agencies, Police staff and other CT teams from all ranks including Image Recovery & Analysis team, Ports, Prevent and Prisons.
External: Work in partnership with NDES, CTU's, CTIU's, SB's, Regional Forces and other external agencies such as CPS, Prosecution, UK and International Intelligence Services, FBI and external suppliers.

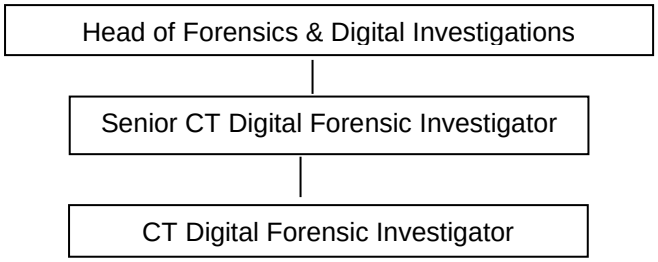
Expertise in Role Required (At selection - Level 1)	**Essential or Desirable**
• Degree in Computer Science/Forensic Computing Studies or equivalent qualification in Digital Forensics and/or significant proven relevant experience/training in these fields.	Essential
• Possess a thorough working knowledge of common operating systems, (Windows, MacOS, Linux) file systems, applications, databases and basic network/Internet technologies.	Essential
• A proven aptitude for problem solving, in a methodical and logical manner.	Essential
• Willingness and ability to attend and successfully complete the Tier 1 core courses in relation to the recovery and analysis of digital evidence, as specified by the National CT Digital Investigations Training Pathway.	Essential
• Ability to work under pressure, make critical decisions and operate to tight schedules and deadlines.	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 digital forensic assistance to investigating officers.	Essential
• Knowledge and understanding of ISO17025, Forensic Science Regulator (FSR) Codes of Conduct and Digital Forensic best practice methodologies.	Desirable
• Practical/proven understanding and/or experience of using forensic software applications for the examination and interrogation of digital devices e.g. EnCase, X-Ways, FTK, XRY, Cellebrite, Oxygen.	Desirable
• Experience in preparing complex reports and statements of evidence.	Desirable
• Willingness and ability to undertake CBRN training and associated activities, including working 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 service.	Desirable
• Has presented or is able to present digital evidence in Court in an effective and professional manner, providing factual and procedural based evidence.	Desirable
Other (Physical, mobility, local conditions)	
• Physical and emotional resilience to deal with abusive and offensive images of extreme violence, obscenity and depravity.	Essential
• Willingness to undergo Psychological Assessments, as and when required.	Essential
• Willingness and ability to travel regionally, nationally & internationally for business purposes, possibly for extended periods and at short notice.	Essential
• Willingness and ability to work unsociable hours, provide 24-hour cover, change hours at short notice and participate in a call-out rota if necessary.	Essential
• Full current UK/European Driving Licence.	Essential

• Successfully undergo MV / SC / vetting procedures.	Essential
• Access to vehicle for Business purposes	Desirable

Expertise in Role - After initial development - Level 2

- Able to interpret, understand and provide detailed explanations of complex Digital Forensics data in a non-technical and accessible manner to SIOs, Investigative Officers, CPS, Prosecution/Defence Barristers and any other audience when required.
- Triaging digital devices on scene to assist in the exhibit seizure process. Communicating any technical issues to the Forensic Management Team, investigating officers and SIOs and other relevant staff.
- Able to operate and display a good working knowledge of a variety of digital forensic hardware and software tools relevant to the role.
- Understand, adhere to and actively promote Digital Forensics best practice methodologies, ISO17025 and ISO17020 standards, FSR Codes of Conduct and the NPCC Guidelines for the examination, analysis and investigation of computers, mobile phones and other digital devices.
- Successfully completed the Tier 1 required courses in relation to the recovery and analysis of digital evidence, as specified by the National CT Digital Investigations Training Pathway.
- Has created and presented Electronic Presentation of Evidence (EPE) court packages including the editing of video and audio data.
- Has presented digital evidence in Court in an effective and professional manner, providing factual and procedural based evidence.
- An understanding of the functions, responsibilities and policies of the CTP NE, WYP, Partner Regional Forces and the National CT Infrastructure.
- Critically impact to the successful disruption, arrest or conviction of offenders through the digital investigation of national/international Terrorism/Domestic Extremism offences and other investigations as required.

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 1 –Practitioner

PART C - DEVELOPMENT OF ROLE

Expertise in Role (Advanced - Level 3)

- Successfully completed the required Tier 2& 3 Specialist courses in relation to the recovery and analysis of digital evidence, as specified by the National CT Digital Investigations Training Pathway.
- Demonstrated expert knowledge and understanding of digital forensic hardware/software, particularly showing an aptitude in a specialist Subject Matter area and potentially achieving a National Subject Matter Expert status in a specialist digital forensic discipline.
- Actively and effectively promote the CT Network, being at the forefront of technical developments within digital forensics.
- Knowledge of network administration and effective data backup technologies and procedures.

- Able to conduct hardware/software validations, maintain accurate records of testing and report findings in relation to ISO17025. Demonstrated higher level of knowledge for ISO17025.
- Demonstrated practical experience in advanced discipline areas such as scripting (SQL, Python), password cracking, device rooting, mobile device eMMC ISP extraction, JTAG, chip-off/on and low level data recovery techniques.

PART D - ACCESS & VETTING

Standard IT Access	Default
Police Building (Perimeter and Zone access)	Perimeter Access to Police Buildings where based
Vetting Level	MV / SC / DV
Date accepted as a role profile	