ROLE PROFILE

Role Title	Regional Cyber Crime Unit Digital Forensic Investigator	**Reporting to**	Senior Digital Forensic Investigator of Yorkshire and Humber Regional Cyber Crime Unit
Section	Yorkshire and Humber Regional Cyber Crime Unit (RCCU)	**District/Department**	Yorkshire and Humber Regional Organised Crime Unit (ROCU)
Tenure		**Rank/Grade**	SO2

Part A – JOB DESCRIPTION

Overall purpose of role	To conduct intelligence led digital forensic investigations on electronic devices, providing expert interpretation of the evidence in a secure format acceptable to the court. Liaison and engagement with investigation teams into serious & organised crime at a local, regional and national level. Actively research and horizon scan for emerging threats to defeat the criminal use of technology by providing methods, processes and software solutions developed in house to mitigate these risks.

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 at a number of stages. This includes the pre executive action phase, attendance at scenes for both proactive and reactive investigation to capture digital evidence/intelligence. The post executive phases/investigation, ensuring that all digital opportunities are explored, sourced and maximised for the timely production of evidence/intelligence in accordance with national guidelines and SIO's Digital Strategy.

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 serious and organised crime. 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. Attend court both nationally and internationally as a subject matter specialist witness. Represent ROCU at CPS Case Conferences, liaising with Prosecution/Defence Barristers, Defence Experts and the Judiciary.

5. Ensure compliance with the 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. Validate and test methodologies developed in house providing compliance with ISO 17025/20.

6. 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 GDPR, RIPA, FOIA, CPIA, PACE and other relevant legislation ensuring compliance at regional, national and international levels.

7. 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.

8. Participate in the assembly, deployment and maintenance of dedicated Digital Forensic Workstations and associated peripherals, equipment and software. Maintain the Regional Digital Forensics Computer Network and attached servers, forensic workstations and review workstations, utlising appropriate support and maintenance, access control, security, updates, upgrades and other administrative tasks.

9. Research and develop solutions to defeat the criminal use of technology through continual professional development and the development of processes and methodologies including the creations of applications / scripts.

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

- Responsible for the mentoring and training of new staff.
- Manage and maintain the ROCU Digital Forensic infrastructure.
- Provide Streamlined Forensic Reports (SFR) and MG11 Witness statements for examinations/analysis undertaken, presenting the evidence/findings to the Investigating Officers, CPS or other requesting agency.
- Work at all times in compliance with the ROCU Departmental policies and procedures, Quality Standards Manual, and Forensic Science Regulator Code of Conduct applicable to Digital Forensics.

Work/Business contacts

Internal: SIOs, Senior Leadership Team, Officer In the Case, ROCU Syndicates, Partner Agencies

External: Work in partnership with ROCU's, National Crime Agency inc NCCU, Regional Forces and other external agencies such as CPS, Prosecution, FBI, Academia, industry partners 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
• 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 ROCU related incidents to provide digital forensic assistance to investigating officers.	Essential
• Knowledge and understanding of ISO17020/17025, Forensic Science Regulator (FSR) Codes of Conduct and Digital Forensic best practice methodologies. Including its application within the laboratory environment and whilst attending scenes; when managing complex investigations and formulating relevant strategies.	Essential
	Desirable
• Practical/proven understanding and/or experience of using forensic software applications for the examination and interrogation of digital devices. Including off the shelf products, for which the Department is accredited, e.g. X-Ways, Axiom, XRY,and Cellebrite and non-accredited software e.g. EnCase, FTK and in house developed applications built to deal with identified challenges and risks	Desirable
	Desirable
• Experience in preparing complex reports and statements of evidence.	
• Has presented or is able to present digital evidence in Court in an effective and professional manner, providing factual and procedural based evidence.	

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

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.

- The ability to examine a broad spectrum of digital devices on scene and/or within the lab to assist in the preservation of data. Communicating any technical issues to the Senior Digital Forensics Investigator, investigating officers and SIOs and other relevant staff. Providing omnicompetent support in the examination of, but not limited to, computers, mobile devices, routers, servers, WAN/LAN networks and volatile data.

- Able to operate and display a good working knowledge of a variety of digital forensic hardware and software tools relevant to the role. Take responsibility for maintaining CPD in these fields.

- 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.

- Has the ability to present 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 ROCU, WYP, Partner Regional Forces and the National ROCU Infrastructure.

- Critically impact to the successful disruption, arrest or conviction of offenders through the digital investigation of serious and organised crime

Structure

```
        ┌─────────────────────────────────────┐
        │        Detective inspector          │
        └──────────────────┬──────────────────┘
             ┌─────────────┴──────────────────┐
             │ Senior Digital Forensic Investigator │
             └─────────────┬──────────────────┘
             ┌─────────────┴──────────────────┐
             │   Digital Forensic Investigator     │
             └─────────────────────────────────┘
```
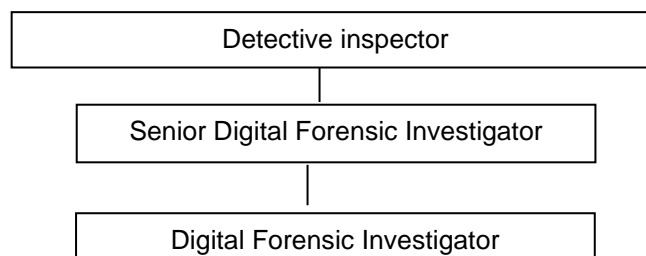
PART B – COMPETENCIES & VALUES

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)

- 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 ROCU 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 ISO17025/20. 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.
- To utilise their skillsets to new methodologies to combat emerging technological threats and share with law enforcement appropriately.

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
Date accepted as a role profile	TBC