Professional Role Profile

Role: Digital Forensic Examiner

Department: Royal Gibraltar Police

Responsible to: Superintendent Crime & Protective Services

JOB PROFILE

To provide professional digital forensic support within the Royal Gibraltar Police by examining digital devices, preserving and analysing electronic evidence, and supporting investigations through the secure handling, interpretation and presentation of digital material.

Key Accountabilities - (This section details the key responsibilities required of the role)

- In consultation with the digital forensics manager, receive, assess, prioritise and process digital forensic submissions in line with operational priorities, evidential standards and force procedures.
- Identify, preserve, recover and analyse digital evidence from computers, mobile devices, storage media and other electronic equipment using approved methods and tools.
- Maintain the integrity, continuity and security of exhibits, audit trails and forensic processes at all stages of examination and evidence handling.
- Provide technical advice to investigating officers and police staff on digital opportunities, evidential risks, device strategy and proportionate forensic approaches.
- Assist with the capture, review and interpretation of digital material relevant to crime investigation, safeguarding, intelligence development and case building.
- Prepare accurate records, forensic notes, schedules, statements and reports suitable for disclosure and supervisory review.
- Give live, verbal testimony in court with clarity, accuracy, and adherence to legal and organisational standards
- Support investigations involving online activity, communications data, imagery, digital media, cyber-enabled offending and the evidential use of electronic devices.
- Work closely with investigators, intelligence staff, prosecutors and partner agencies to ensure digital evidence is understood and effectively incorporated into enquiries.
- Undertake triage, research and prioritisation activity to support timely examination of devices and to identify relevant evidential material efficiently.
- Ensure compliance with legislation, policy, information assurance requirements and recognised digital forensic standards, including data protection and disclosure obligations. Support the secure storage, maintenance and administration of digital forensic equipment, software, systems and evidential materials.
- Keep up to date with developments in digital technology, forensic methods, cyber risks and criminal techniques to maintain professional capability.
- Complete frequent mandatory training and competency updates essential to the role's technical and evidential responsibilities.
- Contribute to continuous improvement, quality assurance and the development of local processes, guidance and good practice within the DFU function.
- Handle distressing, sensitive or explicit digital material professionally and in accordance with welfare, safeguarding and organisational support arrangements.

- Liaise with UK counterparts and external service providers, including preparing and dispatching material for secure transport.
- Undertake any other duties commensurate with the grade of the post as may reasonably be required.

Standards and Behaviours

All RGP staff are expected to understand and act within Our Code of Ethics and Competency and Values Framework (CVF).

COMPETENCY AND VALUES FRAMEWORK (CVF)

The CVF aims to support all policing professionals and sets out recognised behaviours and values which provide a consistent foundation for a range of processes. This framework ensures that there are clear expectations of everyone working in policing which in turn will lead to standards being raised for the benefit and safety of the public.

The CVF has six competencies that are clustered into three groups. Under each competency are three levels that show what behaviours will look like in practice. The table below highlights the levels for this role.

Click here to access the Competency and Values Framework (CVF) document.

Resolute, compassionate and committed	
We are emotionally aware **Level 2**	**We take ownership** **Level 2**
Inclusive, enabling and visionary leadership	
We are collaborative **Level 2**	**We deliver, support and inspire** **Level 2**
Intelligent, creative and informed policing	
We analyse critically **Level 2**	**We are innovative and open-minded** **Level 2**

PERSON SPECIFICATION – DIGITAL FORENSIC UNIT (DFU) OFFICER		
CRITERIA	**ESSENTIAL**	**DESIRABLE**
Qualifications:	• Degree, diploma or recognised professional training in digital forensics, cyber security, computer science, investigative practice or a related discipline, or equivalent relevant practical experience.	• Industry or professional certification in digital forensics, cyber security or information security. • Training in court statement preparation, disclosure or expert evidence. • Training in digital forensic tools, exhibit handling or evidential procedures, or the ability to demonstrate equivalent competence through experience.
Experience:	• Experience of working with digital systems, electronic records, devices or technical evidence in an investigative, forensic, ICT or analytical environment. • Experience of handling sensitive or confidential material accurately and securely. • Experience of maintaining records, audit trails and documentation to evidential or compliance standards. • Experience of working to competing deadlines and prioritising technical or casework activity.	• Experience within policing, criminal justice, government, cyber security or another regulated investigative environment. • Experience of using specialist digital forensic or device examination tools.
Knowledge:	• Knowledge of digital evidence principles, continuity, preservation and the importance of evidential integrity. • Understanding of data protection, disclosure, information security and lawful handling of digital material. • Awareness of cyber-enabled crime, online communications, digital media and the role of digital evidence in criminal investigations. • Commitment to professional development and keeping pace with changes in technology and offending methods.	• Knowledge of policing systems, criminal procedure, safeguarding investigations or wider criminal justice processes.
Key Skills and Behaviours:	• Strong analytical and problem-solving skills, with the ability to examine information methodically and reach sound conclusions. • Good written and verbal communication skills, including the ability to explain technical matters clearly to non-specialists. • Able to work accurately, maintain confidentiality and exercise sound judgement when dealing with sensitive material. • Skilled in the use of Microsoft Office and able to work confidently with digital systems and databases.	• Ability to communicate effectively in Spanish. • Experience of giving evidence or presenting technical findings in formal settings.

	• Able to work independently and as part of a multi-disciplinary team. • Resilient and able to manage exposure to distressing or sensitive material professionally.	
Other requirements:	• Able to attend operational locations, examinations, meetings or court as required. • Able to maintain the required vetting level and comply with force policies relating to digital evidence and security.	•

Required Vetting Level:

Management Vetting (MV)

Management Vetting is a requirement for roles with duties, responsibilities or access that could present an increased risk to the RGP, as designated by the RGP Head of Professional Standards / Information Management & Vetting Manager. Management Vetting (MV) is required for this role due to the postholder's access to sensitive digital evidence, police systems, investigative material and information that requires an enhanced level of trust and assurance.