**GREATER MANCHESTER POLICE**

**JOB DESCRIPTION**

|  |  |
| --- | --- |
| **POST TITLE:** | Digital Forensic Investigator |
| **DEPARTMENT/DIVISION/BRANCH:** | Counter Terrorism Policing North West (CTPNW) |
| **SECTION/UNIT:** | Investigations |
| **GRADE:** | G / I |
| **RESPONSIBLE TO:** | Detective Sergeant, Digital Investigations |
| **RESPONSIBLE FOR:** | N/A |
| **AIM OF JOB:** | To conduct forensic investigations of all digital devices, serving the CTPNW, regional and national requirements. Provide expert professional analysis and interpretation of evidence secured from computers, mobile devices and other storage media in a secure format acceptable to the court.  Responsible for all levels of digital investigations, servicing both Intelligence and Investigation requirements. |

**MAIN DUTIES AND RESPONSIBILITIES**

* To provide expert professional advice to staff within the National Counter Terrorism Network, including GMP and the North West regional forces. Liaise with Police Staff across the National Counter Terrorism Framework and partner agencies including the Security Services and CPS, providing advise in relation to best practice and procedures for Digital Investigations in accordance with nationally agreed protocols, legislation and NPCC Good Practice Guide for Digital Investigations.
* Receive items for examination from the Officer in the case, having first identified what is practical and relevant to investigate, Explain in detail to the SIO / Case Officer what is achievable, ensuring that the submissions forms & exhibit labels have been correctly completed. Undertake a risk assessment of the case and provide an expected target completion date to the SIO / Case Officer.
* Use the computerised job management system for the storage of data relating to that case, whilst maintaining continuity of evidence with the exhibits. Additionally maintain manual files for each case and provide statements in relation to the investigation.
* Deal with telephone enquiries and carry out duties in relation to the unit’s administration.
* Use Forensic software and hardware to recover an image from lawfully seized digital media in accordance with ACPO guidelines and maintain a detailed log outlining steps taken during the process. Where necessary photograph or video proceedings.
* Using forensic software, hardware and validated processes, thoroughly investigate forensic images, maintaining a log of the processes used to obtain evidence, whilst keeping the SIO / Case Officer informed of the progress of the investigation.
* At the conclusion of the case produce a detailed report and statement in a format that is understandable by an individual with limited computer knowledge, whilst ensuring that full disclosure has been provided in accordance with CPIA 2000.
* During the course of the investigation produce an archive copy of any digital evidence onto suitable media, whilst complying with the Data Protection Act.
* Attend searches of major crime or complex crime investigations, as required giving advice on seizing digital media and associated equipment. Where necessary conducting on site examinations of digital media.
* When it is impractical for the SIO / Case Officer to bring exhibits to the unit for examination e.g. business critical systems, attend at the scene and image onsite.
* Where the investigation is of a highly technical and complex nature e.g. hacking and complex server systems, assist the SIO / Case Officer by obtaining a statement from witnesses and questioning the suspect in an interview.
* Maintain the secure property/exhibits store within the unit.
* Attend Court and give evidence as required in the capacity of a Digital Forensic Investigator, who has obtained the necessary accreditation in the forensic procedures and software used during the course of that investigation.
* Keep abreast of all new legislation and procedures that may effect the investigation of Cyber enabled Crime.
* Routinely research new forensic hardware, software and other equipment that may improve the quality and quantity of evidence produced or lead to other improvements in procedures. Maintain and upgrade the office equipment.
* Develop new processes and techniques in line with advancements in technology, ensuring that they are verified and meet accreditation and court standards.
* Responsible for directing, tasking and allocating work to staff.
* To act as a mentor for less experienced members of the unit, providing continuous development and support.
* Provide advice and training to GMP staff, CTPNW staff and other organisations, including briefing senior officers in terrorist investigations.

### General:

* To promote and comply with GMP's policies on health and safety both in the delivery of services and the treatment of others.
* Comply with and promote equality legislation and GMP's policies on diversity and equality. Take steps to eliminate unlawful discrimination, advance equality of opportunity and foster good relations.
* To comply with the requirements of GMP's policies on Drug and Alcohol testing – requirements in respect of specific posts/ roles are described in the policies which are available on the Intranet/SharePoint.
* To fully participate in GMP’s development review process.
* If you have responsibility for staff; to manage staff development, performance and attendance using appropriate GMP policy and procedure
* All staff and officers must adhere to and comply with Data Protection, Freedom of Information and Human Rights legislation and the Authorised Professional Practice (Information Management). It is the responsibility of all staff and officers to maintain data quality and security. Therefore when inputting, updating and using GMP information, you are to ensure that it is Accurate, Adequate, Relevant and Timely (AART), and that it is used / disclosed for business purposes only and kept secure. The most current guidance and advice in respect of compliance with the legislation and information / records management standards can be found on the Information Management Intranet site/Information Services SharePoint site.
* Supervisors and managers have the additional responsibility of ensuring that staff undertake the appropriate training and fully understand and apply the required Force policy, procedures and information / records management standards in the course of their duties. Supervisors and managers should ensure that staff / officers understand their responsibilities in maintaining data quality and security and have appropriate processes in place to monitor compliance.
* To carry out such other duties which are consistent with the nature, responsibilitiesand grading of the post.

**NOTES**

This job description records the principal responsibilities of the job at the date shown. The job description will be updated from time to time in conjunction with the post holders to reflect changes.

Please note that we will consider making reasonable adjustments to the above, in line with the Equality Act.

The most up to date version of various GMP policies and pieces of legislation can be found on the Intranet/ SharePoint.  Further support and guidance can be sought from the HR Advisory Service or the Information Compliance and Records Management Unit. The most up to date telephone numbers are available on the GMP Intranet.

**LEADERSHIP EXPECTATIONS**

The Leadership Expectations is a framework, which describes the attributes, behaviours, and outcomes that are demonstrated by successful leaders across GMP. They also describe what all our staff and officers need to deliver in order to achieve the Force’s vision of “Protecting society and keeping people safe”.

The Leadership Expectations will be embedded in leadership training, recruitment and selection, police officer promotion, development programmes and performance reviews.

**Our Leadership Expectations are:**

# Inspiring Others

Listening to, involving and motivating others to take action and behave with courage and integrity  
  
**Enabling Change and Improvement**  
Taking responsibility to solve problems, implement change and make improvements to our services  
  
**Developing Yourself and Others**  
Developing yourself and others to succeed and increase their contribution to GMP  
  
**Responsibility for/to the Team**

Setting a clear direction and promoting teamwork to achieve high standards of professionalism and performance in all situations however challenging  
  
**Working in Partnership**Working as one GMP team and with external partners to achieve results that benefit GMP and our communities  
 **Demonstrating Respect and Compassion**Treating all our people, partners and communities with respect and compassion  
  
**Service Delivery**  
Delivering excellent policing services to the people of Greater Manchester

**Leaders have been identified at four levels:**

* Peer
* First
* Middle
* Senior

The **Digital Forensic Investigator** has been identified as: **A Peer Leader**

**Please Note**: As well as assessing candidates against criteria outlined in the Person Specification, the selection process will also include candidate assessment of the leadership expectations.

For more information on our leadership expectations please visit our website

www.gmp-recruitment.

**PERSON SPECIFICATION**

**Digital Forensic Investigator**

**CTPNW**

|  |  |  |
| --- | --- | --- |
| **Short-Listing Criteria** | **Essential/**  **Desirable**  **(E/D)** | **Assessment of Criteria (how the shortlisting criteria will be assessed)** |
| **Qualifications/Education**  **Grade G**  Obtained a degree in Digital Forensics or similar.  or  Has relevant experience and can demonstrate the same level of knowledge/training.  Prepared to undertake certification in the following areas once in post;   * Forensic Foundations * Internet forensics * Network Forensics * Mobile forensics     **Grade H**  As for Grade G plus;  Post Graduate Certification or Bachelors Degree in Digital Forensics or similar.  Achieved certification in the following areas;   * Forensic Foundations * Internet forensics * Network Forensics * Mobile forensics   Trained in the following software’s;   * Encase Forensics * X-ways * XRY * UFED   Attended training course in Live Forensics.  **Grade I**  As for Grade H plus;  Completed advanced training or certification in Forensic Software's.  Training in SQL, computer programming or network administration. | E  E  E  E  E  E  E  D | AF(C)  AF(C)  AF(C)  AF(C)  AF(C)  AF(C)  AF(C)  AF(C) |

|  |  |  |
| --- | --- | --- |
| **Experience**  **Grade G**  Experience in the IT Industry using a full range of both client and server based operating systems with industry accredited computing related certification.  Experience of using forensic software applications and other software packages, including programming.**\***  Prior Investigative employment  Background. \*  Experience in mobile data extraction tools and producing evidential packages. \*  **Grade H**  As for Grade G plus;  Experience working in digital forensic investigations or in a technical digital role.  Experience in training and mentoring staff.  Experience in recognising and dealing with risk in a digital environment.  Experience in briefing and communicating digital forensic methods and results to other departments and agencies.  Experience of dealing with complex digital investigations.  **Grade I**  As for Grade H plus;  Experience of working with SIO's and Case Officers in directing investigative strategy for CT related Investigations.  Experience in prioritisation of investigative strategies and managing the associated risks.  Experience of conducting numerous complex digital forensic investigations, managing workload and prioritising tasks accordingly.  Experience of presenting evidence at Court.  Experience of managing and tasking staff during CT digital Investigations. | E  D  D  D  E  D  D  E  E  E  E  E  D  E | AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I |
| **Knowledge**  **Grade G**  Thorough working knowledge of computer Operating Systems.  In-depth Knowledge of computer networks.    Knowledge of Unix Operating Systems. **\***  An understanding of legislation e.g. Computer Misuse Act, RIPA & PACE. **\***  **Grade H/I**  As for Grade G plus;  Knowledge and Understanding of the ACPO Good Practice Guide for dealing with Digital Evidence.  Thorough working knowledge and understanding of a variety of digital devices, including computers and mobile devices.  Thorough understanding of the importance of lawful seizure, exhibit handling and continual integrity of exhibits throughout an investigation.  Thorough understanding of the file preparation process and disclosure procedures. | E  E  D  D  E  E  E  E | I  I  I  I  AF/I  AF/I  AF/I  AF/I |

|  |  |  |
| --- | --- | --- |
| **Skills/Abilities**  **Grade G**  The ability to identify component parts of computers and understand their functions.  Able to deal with lengthy or tedious enquiries and analyse the data content, producing concise accurate reports.    Capable of maintaining confidentiality.  Ability to deal with serious or potentially disturbing material.  Ability to convey technical information in a manner understandable to the audience.  Excellent interpersonal skills and ability to communicate on a variety of levels across the organisation and outside agencies.  Able to undertake low level investigations while being mentored/ supervised.  Produce reports and statements for low level investigations.  Able to undertake low level/non complex investigations without supervision.  **Grade H**  ***As for Grade G plus:***  Able to carry out High Level/more complex investigations with supervision.  Produce reports and statements for more complex /high level investigations.  **Grade I**  As for Grade H plus;  Able to carry out high level/complex investigations without supervision.  Produce reports and statements for high level / complex investigations. | E  E  E  E  E  E  E  E  E  E  E  E  E | AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I  AF/I |
| Other **Grade G/H/I**  Has achieved a good attendance record.  Full driving licence and access to a vehicle for business purposes.  Willing to attend Police basic driving course to allow use of Police Vehicles for work purposes.  Willing to participate in a standby scheme where staff are on call on a rota basis.  Willing to work out of the GMP force area to conduct the role, regionally, nationally and internationally.  This is a designated post under the Force Vetting Strategy and the post will therefore attract an enhanced level of vetting.  Willingness to participate in a psychological screening assessment process. | E  E  E  E  E  E  E | AF(E)  AF(C)  AF/I  AF/I  AF/I  AF/I  AF/I |

Note: Progression to grades H and I will be subject to successful assessment of competence.

**Key**

|  |  |
| --- | --- |
| **AF(E)** | **Eligibility (this will be checked by the recruitment team)** |
| **AF** | **Application Form** |
| **C** | **Certificate** |
| **T** | **Test** |
| **I** | **Interview** |

**Please note:**

* Candidates who do not demonstrate on the application form, criteria assessed at eligibility stage (E), may not be considered for short-listing.
* Candidates who do not demonstrate on the application form, criteria identified as essential and being assessed at application form (AF), may not be shortlisted.
* All essential criteria above will also be discussed in GMP’s - development review process.
* The desirable criteria marked with an asterisk will be desirable at selection stage but will become essential once in post and will be discussed in the development review process.
* A good attendance record will be assessed in accordance with current guidelines. For recruitment purposes this can only legally occur following a provisional offer, at which stage the offer can be rescinded. Consideration will be given to Disability related absence/maternity related absence in line with current guidelines.