Job description

Title:	**Digital Investigation Specialist**
Reports to:	**Digital Investigation Unit Manager (within DMI)**
Location:	**Any IOPC office**
Grade:	**11**
Salary:	**£36,150 per annum plus London Weighting £4,731 if based in Canary Wharf or Croydon**
Contract:	**Permanent**

Purpose

As a Digital Investigation Specialist, you will be welcomed into a dynamic and inclusive DMI department. The IOPC is on a journey to develop its culture, perspectives and ethos to support the organisation's core outcomes and this is your opportunity to enter into the varied world of IOPC Operations, allowing you to develop your mindset and approaches to contribute to improving the police complaints system in England and Wales.

The IOPC exists to investigate complaints fairly and thoroughly. The IOPC has the power to initiate, carry out and oversee investigations. It is also responsible for monitoring the way complaints are handled by local police forces.

The purpose of the role of Digital Investigation Specialist (DIS) is to work as part of a national dedicated digital team, using their digital expertise to enhance IOPC investigations, providing advice and guidance to Investigations colleagues on the collection, review, and presentation of digital evidence.

The DIS will provide technical expertise on cyber-digital investigation issues encountered by Lead Investigators during IOPC investigations, coordinate digital submissions to external forensic suppliers, and where appropriate to conduct digital review of devices and associated download material to produce evidential material for use in proceedings

The DIS will also support the DIU Manager, within the agreed sign off structure within DMI in strategic initiatives, to achieve operational objectives.

Key Relationships:

- Internal - National Operations colleagues, Procurement, ICT, Quality and Service Improvement team, Intelligence Unit, Learning & Development, Legal, Policy
- External - Police Digital Forensic Unit's, including their senior leadership teams, PONI, GSOC, PIRC, NTAC, digital forensic providers, College of Policing, Forensic Science Regulator

The post holder will work closely with internal and external stakeholders at all levels.

In performing this role, you will have repeated exposure to distressing material which will likely be impactful, traumatic and challenging. Examples of the types of material you may encounter include: violent death scenes, child sexual abuse, domestic violence, sexual offences, extreme pornography – this is not an exhaustive list. Given the nature of the work, it is also very likely that you will have extended contact with individuals who are experiencing extreme distress. The IOPC recognises this and offers all staff a range of wellbeing provisions, including TRiM (Trauma Risk Management) peer-to-peer support, a dedicated Wellbeing Advisor, and access to free confidential counselling. All staff are strongly encouraged to proactively access and engage with the support available. If you would like to speak about this element of the role with somebody already doing similar work at the IOPC, please contact Lucy Thompson, DIU Manager and this can be arranged.

Organisational context

We work in the context of our agreed values which inform the way we do things at the IOPC. The Digital Investigation Specialist will need to be commited to managing in the context of these values.

Seeking truth

We feel privileged to be the custodians of the police complaints system. We value the trust of the public and police and commit to being just and fair in uncovering the truth. We recognise that a just outcome relies on being unbiased and transparent in getting to the truth of what happened.

Being inclusive

We have an inclusive culture. We are fair and impartial in our treatment of all individuals. We work across boundaries, both internal and external, collaborating and building strong relationships.

Empowering people

We believe everyone should be a leader and play a part in shaping the direction of the organisation. We provide a supportive and challenging environment where people can thrive and reach their potential. We trust our people to do the right things. We encourage calculated risk taking and evidence-based decision making. Where genuine mistakes are made, we will support people and identify opportunities for learning and improvement. We ensure that people can make complaints without experiencing unfair treatment.

Being tenacious

Our work requires us to be bold, resilient and committed to making a difference to the public. We take our duties as public servants to heart and our dedication is reflected in our work. We meet the challenges with perserverance to attain individual and organisational goals.

Making a difference

The value of our work is not defined solely by volume, but by the impact our work has on policing and public confidence. We define quality by how well our work meets the service user needs. We will focus our efforts on areas that will make a difference to our communities.

The IOPC is committed to **promoting equality and valuing diversity** in everything we do. Our vision is to be, and to be seen as, a leader in inclusive employment and services, demonstrating this ethos in everything that we do.

- As a silver standard Stonewall employer, we continue to commit ourselves to being a LGBTQ+ employer through the work of our Pride LGBTQ+ Staff Network, creating welcoming environments for lesbian, gay, bi and queer people.
- We are pleased to share we are a signatory of the Business in the Community Race at Work Charter. The Charter is composed of five calls to action for leaders and organisations across all sectors.
- Being a Disability Confident employer, the IOPC is dedicated to removing the barrier for disabled people to thrive in the workplace.
- Our Staff Networks are constantly working to make the IOPC the leaders of inclusive employment, from our Allyship Programme to Operation Hotton, to Welsh Language Standards and Know the Line Policy, we are constantly seeking new ways to create an environment for all to develop and thrive.

Main duties and responsibilities

- Provide an expert specialist function in the end-to-end investigative process by identifying digital opportunities, recovering evidence, managing forensic submissions, reviewing key evidence, and producing investigative material to deliver against lines of enquiry.
- Deliver a specialist operational capability at incident scenes, providing strategic oversight, coordination of resources and taking ownership to preserve and recover digital evidence in accordance with national standards and good practice.
- Produce reports and statements in relation to specialised, technical digital lines of enquiry and explain these findings in proceedings when required (including expert testimony if qualified and authorised when required).
- Design and deliver comprehensive training programs to enhance the digital investigation capabilities of staff at all levels, fostering a culture of continuous professional development.
- Develop, implement, and oversee digital investigation policies and procedures, ensuring they are up to date with the latest legislation, technology, and best practices in collaboration with relevant internal and external stakeholders.

- Engage with internal and external stakeholders to provide advice and explanation of digital investigation techniques, evidence, products, and policy.
- Deliver a high-quality, efficient, and cost-effective service to investigations – offering technically sound, evidence-based advice and challenge, including to senior staff.
- Provide strategic oversight and coordination of digital forensic operations, ensuring effective resource management and high-quality outcomes.
- Work with a range of internal and external stakeholders to ensure legal compliance, drive continuous improvement and IOPC effectiveness in cyber-digital capabilities.
- Take responsibility for developing and maintaining knowledge of technological, legislative, social, and political developments in the cyber-digital arena.
- Conduct comprehensive reviews and quality assurance of digital investigation processes, providing detailed reports and actionable recommendations to senior leadership to drive continuous improvement.
- Horizon scanning and identifying future changes to the operations manual, policy and procedure.
- Build and maintain appropriate professional relationships with relevant stakeholders to ensure that IOPC understanding of relevant legislation and policy remains current, in line with emerging technologies and best practice.
- Assess, report and act on threat, harm and risk posed to IOPC investigations nationally through changes in technology, legislation, policies, or patterns in offending.
- Utilise specialist knowledge to develop in-depth digital investigation strategies, identifying lines of enquiry whilst ensuring practices align with policy and legislation.
- Regularly update senior leadership and key stakeholders on the progress of digital investigations through detailed reports and presentations, ensuring transparency and informed decision-making.
- Identify opportunities for cross-departmental working, providing advice and signposting investigators to internal and external stakeholders as required.
- Assist operational investigators with the identification, recovery, and presentation of digital evidence to ensure that investigative outcomes are achieved.
- Drive and support advancements in DIU, the wider organisation, and the police complaints system by actively participating in a wide variety of working groups with both internal and external stakeholders.
- Drive to promote innovation and improvements to quality and standards, to achieve and maintain investigative excellence.
- Recover, present, and utilise cyber-digital evidence during investigations in accordance with policy and national good practice.

- Act as a single point of contact for the IOPC to plan, manage and process digital forensic submissions with external suppliers/Digital Forensic Units, and manage/maintain these relationships.
- Attain and maintain specialist training and accreditation, driving personal development in line with the technical requirements of the role.
- Lead and manage strategic initiatives and projects related to digital evidence recovery and presentation, ensuring alignment with organisational goals and compliance with national standards.
- Quality assure the storage and management of digital material obtained by the IOPC, ensuring its integrity in line with IOPC policy and security standards.
- Provide expertise both internally and externally surrounding cyber-digital evidence in IOPC investigations, managing risk and maximising opportunities.
- Develop knowledge of and utilise specialist forensic software to extract and review digital evidence, delivering usable products to stakeholders against lines of enquiry.
- Quality assure peer produced evidential products and provide constructive feedback within established quality review processes.
- Reviewing digital actions undertaken by external bodies and advising on their proportionality and appropriateness.
- Undertake proactive research into the latest hardware and software products, techniques, and good practice available, including applications, and assess how they may support IOPC investigations and make recommendations.
- Promote the effective use of digital technology in the police complaints system, supporting learning recommendations and organisational policy.
- Proactively identify and report on threats and opportunities to the IOPC's cyber-digital investigation capability.
- Develop and maintain an expert working knowledge of the DEMS system to effectively manage digital evidence and support business requirements.
- Provide specialist advice/expertise on appropriate wording regarding digital evidence to investigators for use in, for example, warrant applications, search briefings, etc.
- Employ an investigative mindset whilst reviewing digital evidence, informing Lead Investigators of potential further offences or conduct issues where applicable.
- Represent the DIU in meetings with external bodies, including CPS, to provide digital expertise.
- Utilise specialist knowledge and forensic tools to access and remediate subject devices, ensuring the secure and complete deletion of unauthorised or illegal digital materials, including images, videos, contacts, and messages, in compliance with legal and ethical standards.
- Assist the Directorate of Major Investigations and the Operations Directorate in achieving its key deliverables.

Your focus:

- Delivery of high-quality advice and expertise to support digital investigations, demonstrating IOPC core values in every aspect of the role.
- Providing subject matter knowledge to support to the IOPC strategic objectives.
- Developing yourself to achieve personal and organisational objectives.
- Maintain professional expertise through continual professional development including changes to technology, policy, and legislation.
- Act as an agent of change, utilising innovation, and creativity to drive continuous improvement in service delivery.

Person specification

Essential

- Investigative experience and to hold relevant IOPC accreditation or an equivalent investigative accreditation.
- Driving licence valid for driving in England & Wales.
- Good general education or demonstrated through structured workplace development.
- Experience and/or knowledge of digital investigations.
- Evidence of effective oral and written communication skills, including report writing.
- Delivering a high standard of work within demanding timescales.
- Identification of operational and organisational risk.
- Working effectively in a changing environment.
- Stakeholder negotiation and influencing.
- Highly developed IT skills including use of MS Word and MS Excel.
- Experience processing digital evidence in accordance with relevant policy and guidance.

Desirable Experience

- Experience of using digital forensic software, such as Cellebrite Reader, XRY and XAMN.
- Experience of attending searches/arrests where digital evidence has been relevant.
- Experience of liaising with complainants, vulnerable victims and subjects to obtain digital evidence.
- Experience in providing evidence-based advice and challenge to senior staff.

- Experience in developing strategies, standards, procedures, policies, and guidance.
- Knowledge and understanding of the IOPC's operational work, including referrals and investigations.

Skills and Abilities

- Ability to show initiative and adapt in a changing environment.
- Ability to recognise the development needs of yourself and be proactive in addressing them.
- Ability to prioritise and manage tasks effectively to deliver quality outcomes within demanding timescales.
- Ability to work effectively in a team with diverse ideas and people.
- Ability to communicate effectively both verbally and in writing and adapt communication styles as appropriate.
- Ability to analyse complex information, identify the key issues and make recommendations.
- Ability to identify and respond to the diverse needs of individual and stakeholder groups.

Technical Competence

- Ability to use specialist software relating to cyber-digital investigations to extract, analyse and report on data.
- Have knowledge and understanding of the law and procedure in connection with the following areas:
    - Digital Forensics
    - Network investigations
    - Digital exploitation
    - Wi-Fi Opportunities
    - Open-source research
    - Communications data
    - ANPR
    - CCTV

- Key legislative knowledge of:
    - PACE
    - CPIA including PII
    - ECHR
    - FSR
    - Data Protection
    - IP act 2016
    - RIPA 2000 Part 3

Successful candidates will need to complete relevant training and work towards a recognised accreditation such as ICDIP.

Reasonable adjustments

The IOPC is a diverse and inclusive workplace and we want to help you demonstrate your full potential whatever type of assessment is used. We are open to providing you with the tools you need to succeed, from extra time to formatting changes, to name a mere few. If you require any reasonable adjustments to our recruitment process, please email humanresources@policeconduct.gov.uk

Working conditions

Making the IOPC a great place to work is one of our key priorities. We are pleased to offer a unique hybrid working model based on business needs, balanced with the needs of our colleagues. Our business need framework guides our decisions about when it is best to work onsite (in our offices or other appropriate locations) to complete tasks most effectively or when to work remotely, offering colleagues flexibility to work where they feel most productive and supporting work-life balance. The model also encourages staff to feel welcome at the IOPC by ensuring we have opportunities to work face-to-face as teams.

Preparation checklist

- ☐ Review the full job description
- ☐ Review the behaviours and the descriptors for each behaviour
- ☐ Review the Strengths dictionary
- ☐ Review the IOPC values
- ☐ Consider your Strengths (if applicable)
- ☐ Consider drafting example answers that cover the specific elements
- ☐ Prepare some questions to ask the interviewers