**Job description**

**Title: Digital Investigation Specialist**

**Reports to: Digital Investigation Unit Manager (within DMI)**

**Location: Any IOPC office**

**Grade: 11**

**Salary: £33,783 (plus £4,438 London Weighting, if applicable)**

**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.

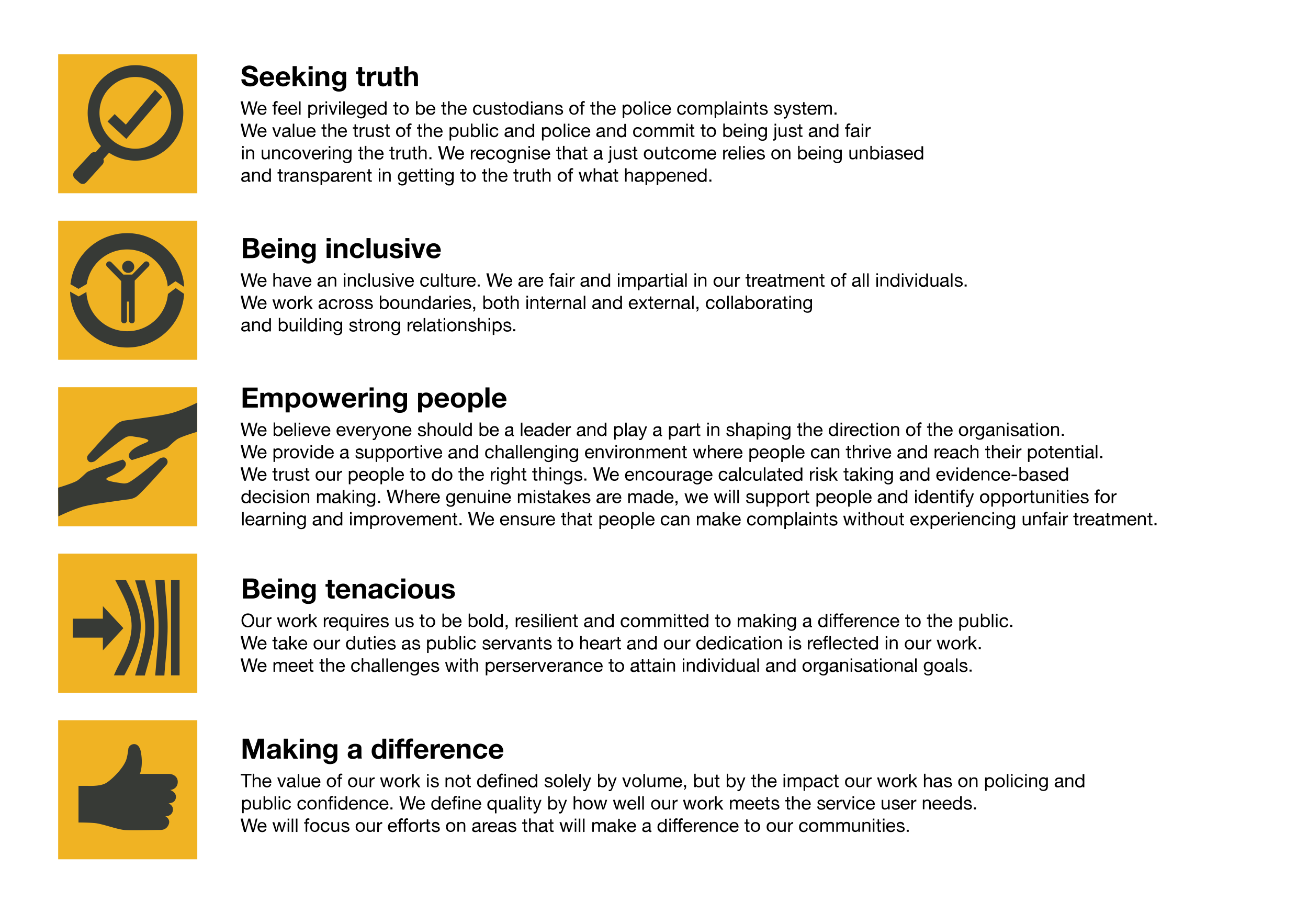
The IOPC exists to investigate complaints fairly and thoroughly. The IOPC has the power to initiate, carry out and oversee investigations. It is also responsible for monitoring the way complaints are handled by local police forces.

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.

# 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.

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](https://race.bitc.org.uk/issues/racecharter) 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](https://www.policeconduct.gov.uk/recommendations/operation-hotton-recommendations-metropolitan-police-service-september-2021), to [Welsh Language Standards](https://www.policeconduct.gov.uk/who-we-are/equality-and-diversity/welsh-language-standards) and Know the Line Policy, we are constantly seeking new ways to create an environment for all to develop and thrive.

***Text

Description automatically generated with low confidenceGraphical user interface, text, application

Description automatically generatedShape

Description automatically generated with medium confidence***

# Main duties and responsibilities

* Support 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.
* Provide expertise internally surrounding cyber-digital evidence in IOPC investigations, managing risk and maximising opportunities.
* Assess and report on threat, harm and risk posed to IOPC investigations nationally through changes in technology, legislation, policies, or patterns in offending. Work collaboratively with the strategic lead to ensure continuous improvement and IOPC effectiveness in cyber-digital capabilities.
* Take ownership for identifying and delivering learning and development opportunities for enhancing IOPC digital capabilities.
* Build and maintain appropriate professional relationships with relevant stakeholders to ensure that IOPC understanding of relevant legislation and policy remains current.
* Contribute to policy/process development to reflect emerging changes in legislation, technology, codes of practise and guidance.
* Work collaboratively to promote innovation and improvements to quality and standards, to achieve and maintain investigative excellence.
* Engage with external stakeholders to provide advice and explanation of digital investigation techniques, evidence, products, and policy.
* Quality assure the management of digital material throughout its lifecycle to ensure the organisational process has integrity.
* Attend proceedings and provide evidence, (including expert testimony if qualified and authorised when required.)
* Deliver a high-quality, efficient, and cost-effective service to investigations with a significant digital element – offering technically sound, evidence-based advice and challenge, including to senior staff.
* Provide operational advice on cyber-digital lines of enquiry, managing risk and maximising opportunities.
* Deliver a specialist operational capability at incident scenes, taking ownership to preserve and recover digital evidence in accordance with national standards and good practice.
* Recover, present, and utilise cyber-digital evidence during investigations in accordance with policy and national good practice.
* Produce reports and statements in relation to specialised, technical digital lines of enquiry and explain these findings in proceedings when required.
* Act as a single point of contact for the IOPC to plan, manage and process digital forensic submissions with external suppliers.
* Utilise specialist forensic software to extract and review key evidence, delivering against lines of enquiry.
* Ensure that digital material obtained by the IOPC is stored and managed in line with IOPC policy and security standards.
* Identify and report on threats and opportunities to the IOPC’s cyber-digital investigation capability.
* Take responsibility for developing and maintaining knowledge of technological, legislative, social, and political developments in your business area
* Assist the DIU manager to support the knowledge and development of IOPC staff at all levels in the cyber-digital arena.
* 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.
* Undertake specialist training and accreditation in line with the technical requirements of the role.
* Promote the effective use of digital technology in the police complaints system, supporting learning recommendations and organisational policy.
* Assist 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.

## Experience

* 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.
* Experience processing digital evidence in accordance with relevant policy and guidance.

## 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
  + 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](mailto: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