THAMES VALLEY POLICE

DETECTIVE CONSTABLE ROLE SPECIFICATION

Role Title:	Detective Constable – Regional Prevent Officer	Department:	Regional Cyber Prevent
Reports To:	Regional Cyber Protect/Prevent Sergeant	Location:	'Agile'

Purpose of role:	The role holder will ensure that the national cyber prevent strategy is represented in SEROCU activity. They will build and develop relationships with regional and local stakeholders and partners in the public and private sectors to develop and deliver Prevent priorities. The role holder will engage with offenders and individuals referred to the Regional Cyber Prevent team to divert and educate to prevent offending. The role holder will use interview techniques to secure intelligence and better understanding of cybercrime offending. The role holder will build relationships with partners to promote awareness and understanding of cyber offending and pathways into cybercrime to increase referrals into the Regional Prevent team for engagement.
Principle Responsibilities:	
	Tactical Prevent Activity and offender management: • Prevent SPOC for all NCCU and ROCU led coordinated operations undertaking the delivery of timely interventions such as cease and desist activity, diversions, offender management, mentoring etc. • On-going local identification of individuals on the periphery of cybercrime. SPOC for business as usual Prevent intelligence packages from NCCU, Action Fraud and ROCU's for the delivery of interventions. • Working closely with ROCU investigation and local/regional HUMINT teams to identify local and regional Prevent opportunities. • On-going management/monitoring of all subjects to prevent re-offending, including advising on conditional cautions and working with Safeguarding/YOTs/CPS/probation to ensure positive diversion options are understood and implemented.

	Intelligence collection: • Intelligence collection about the scale of the threat at regional/local level, age of offenders, problems in schools, links to neurodiversity etc. Ensuring all local Prevent intelligence is recorded and reported back to forces and NCCU Prevent. • Undertake Prevent intelligence interviews with offenders post disposal to build knowledge on pathways into cybercrime in line with national Prevent intelligence requirements. • Working closely with local force cyber prevent or prevention teams to build local intelligence and identify Prevent opportunities.
	Partnership working: • Identify and build partnerships with local industry, education and third sector partners to promote the Prevent message and identify initiatives in the region that can provide an alternative to cybercrime and towards which Prevent subjects can be diverted. • Design and develop events for the public, raising awareness around Computer Misuse Act offences and sending general Prevent message to relevant target audiences. • Support NCCU Prevent objectives with academia to build insight into offender pathways and improve strategy.
	Communications: • SPOC for all NCCU led cyber Prevent campaigns including Cyber choices and operations. • Provide Prevent advice and publicise correct Prevent resources (NCCU cyber choices media and leaflets, lesson plans) to schools, parents and other carers or education or local authorities.
	Measurement of impact • Follow measurement of performance and impact regime established by NCCU Prevent.
	Support to NCCU Prevent project and operational support: • Where required, leading or supporting on the design and delivery of NCCU Prevent strategy, projects and operations in line with the national cyber Forward Work plan priorities. Current priorities are offender management and diversion, the Cyber choices campaign, Gaming, Neurodiversity, international Prevent and criminal marketplace disruption.

Essential role based training:	N/A
Essential Criteria:	- Demonstrates experience of investigation, interviewing and intelligence skills (Essential) - Strong organisation and project management skills. (Essential) - Stakeholder and relationship management skills (Essential) - Experience of assessing and managing threat/harm/risk (Essential) - Good communication skills (Essential) - Proficient in the use of office IT systems (Essential)
Desirable Criteria:	- Intelligence debriefing skills. (Desirable) - Experience or understanding of cybercrime (Desirable) - Experience of offender management (Desirable) - Experience of influence or behaviour change activity or behavioural science (Desirable) - Understanding of the impact of neuro-diversity in policing (Desirable) - Interest in cyber, computing and technology (Desirable)
Competency Value Framework (CVF) – Level 1 The role holder should effectively deliver these key requirements.	- We are emotionally aware – level 1 - We take ownership – level 1 - We collaborate – level 1 - We deliver, support and inspire – level 1 - We analyse critically – level 1 - We are innovative and open-minded – level 1
Additional Information:	N/A