Job Evaluation Number	B671

JOB DESCRIPTION

Job Title: Information Governance Officer	
Job Family: Business Support	**Role Profile Title:** BB3 Police Staff
Reports To: Information Governance Manager	**Band level:** 3G – Entry level 3H – Proficient
Staff Responsibilities (direct line management of): Nil	

a. **OVERALL PURPOSE OF THE ROLE**: Defines the role, put simply, why it exists.

The overall purpose of the role is to: provide data protection, General Data Protection Regulation (GDPR), law enforcement processing and information governance expertise to advise and instruct officers, staff and project teams to ensure legislative compliance and enable the delivery of information management strategy, policy and procedures across both forces. Providing support and advice to the Data Protection Officer.

b. **KEY ACCOUNTABILITY AREAS**: Define the important aspects of the role for which the job holder is responsible for results or outcomes.

The key result areas in the role are as follows:
1. Lead change project teams through completion of Data Protection Impact Assessments (DPIA), assessing how well proposed new initiatives will comply with the GDPR and Data Protection Act, recommending and negotiating the agreement of pragmatic risk mitigation solutions, producing the DPIA Report and briefing the Data Protection Officer. Work in collaboration with Procurement Teams to ensure that contracts contain the necessary data protection safeguards via recommended contract clauses, particularly where data processing is outsourced and / or involves international transfers of personal data. Assess ICT applications for use of personal data in the testing of new IT systems and instructing how much personal data is proportionate to use in order to balance data protection act compliance, whilst ensuring sufficient testing can take place. Recommend approval of applications and identify any mitigating activity to be taken.
2. Support and advise Senior Leaders in the organisation (as Data Guardians and Information Asset Owners), in the management of their information risks by assessing their compliance with the GDPR and Data Protection Act, recommending and negotiating agreeable mitigating actions and production of a Risk Discovery Report. Provide ongoing support by meeting Data Guardians to provide 4 monthly horizon scanning updates and reviews of outstanding risks. Develop strong relationships with senior managers / officers, who are data owners, to increase their awareness about existing and emerging information risks, influence them to increase their participation in helping the two forces' adhere to the GDPR and Data Protection Act and, more broadly, raise the profile of data protection across the two forces.
3. Instruct data security incident investigators to take the appropriate action required to limit circulation of personal data and minimise any subsequent detriment to individuals. Propose future preventative measures, recommending whether the incident meets the legal threshold to notify the Information Commissioner's Office and if so preparing the necessary report, and ensuring incident is correctly classified and rationale recorded.

4. Assess compliance of proposed sharing initiatives and advising internal and external customers on how new information sharing processes / relationships should be set up lawfully, producing appropriate governance documentation (Information Sharing Agreements and Data Processing Contracts) and maintaining an accurate record of data use within the Information Asset Register.
5. Assess police records in accordance with the statutory 'Management of Police Information' retention framework to decide the future retention or deletion of offender records and deleting any relevant records. Where records are retained ensuring inaccurate or duplicated information are amended appropriately and creating auditable records of activities carried out.
6. Advise internal customers and external customers (such as partner agencies) on adhoc queries on GDPR, data protection and all information governance related activities, solving related data use and sharing problems, providing recommendations and outcomes to resolve issues and mitigate risks. Involves research of various external sources / material to interpret the practical application of new legislation where as yet there is no case law to refer to. Create 'good practice' data protection and information management guidance for force staff, and the design and delivery of data protection training to officers and staff of varying ranks, enabling departments and other teams to take ownership of data protection compliance in their departments.
7. Conduct audits as required to ensure personal data is used only for a justified / lawful purpose and complies with the GDPR and Data Protection Act.
8. Train and transfer expertise to new staff within the Information Governance Team to achieve resilience and continual professional development.

c. **DIMENSIONS**: Include matters such as key result areas that make the greatest demands on the role holder, seasonal pressures, items processed, the number of customers and/or level of authority to make financial decisions or commit other resources.

Further Comments:
Influencing and negotiating with senior leaders to prioritise the necessary money and resources in order to comply with the GDPR and Data Protection Act, where failure to do so could ultimately attract fines from the Information Commissioner's Office (maximum of £17 million).
Researching and staying up to date with expertise of the GDPR / Data Protection Act, and experience of how to apply it practically is fundamental to balancing legislative compliance and maximising business benefits where these two factors can often be conflicting.
Managing and balancing a variety of tasks and the needs of multiple customers at any one time, where it will be necessary to make risk based assessments to determine which customer's requests take priority.
The review of offender records will involve reading material that describes the nature of offending ranging from minor to serious offences.
Delivering services and advice to two forces with different structures, policies, cultures and systems.
Be prepared to provide resilience between both Forces and ability to travel occasionally when required.

d. **CHARACTERISTICS OF THE ROLE**

Expertise: Concerned with the level of administrative, professional and/or technical expertise (knowledge and skills) needed to perform the role effectively; may be acquired through experience, specialised training, and/or professional or specialist education and training.

The knowledge or skills required in the role are as follows (essential or desirable): 3G – Entry level	***E/D***
1. Excellent problem solving skills including the ability to understand customer requirements, work within 'shades of grey' and objectively assess risk and recommend pragmatic solutions.	E
2. Ability to pay attention to detail and work within and apply formal / legal frameworks to a wide variety of situations.	E
3. Ability to communicate confidently and effectively with both junior and senior ranking officers / staff and explain technical matters in a user friendly way; whether verbally, in written guidance or delivering presentations.	E
4. Ability to take ownership of delivering outcomes, working under own initiative to manage and prioritise fluid workloads.	E
5. Ability to influence people who may not share your views or priorities to find acceptable solutions and mitigations to data compliance issues.	E
6. Experience of working in an information governance or data protection role or holding an information management qualification.	D
In addition to the entry level requirements, the knowledge or skills required at the 3H proficient level are as follows (essential or desirable):	***E/D***
7. Has an effective working knowledge of the UK GDPR and Data Protection Act 2018 provisions (in particular Part 3 – processing for the law enforcement purpose) and is able to apply them appropriately to real life policing scenarios.	E
8. Has achieved competency sign off in all of the Primary Thames Valley Police and Hampshire Constabulary Information Governance function training modules.	E
9. Ability to independently manage a full caseload of Information Governance work with minimal supervision and use own initiative when problem solving.	E
10. Take a proactive role in developing their own data protection knowledge.	E