

 **NHS NATIONAL SERVICES SCOTLAND**

# JOB DESCRIPTION

|  |
| --- |
| **1. JOB DETAILS** |
| The following provides guidance on development of Job Descriptions. This guidance should be used when completing the Job Description Template. |
| Job Title | **Information Governance Advisor** |
| Immediate Senior Officer/ Line Manager | NSS Senior Consultant Information Governance |
| Department | Information Security and Governance |
| SBU | Digital and Security |
| Location |  |
| CAJE Reference | NPITG536 |

|  |
| --- |
| **2. JOB PURPOSE** |
| To support the implementation in all aspects of data protection, privacy, information sharing and related issues across Digital and Security, NSS and national when required. Supports the delivery and development of all information governance matters across Digital and Security and NSS, promoting best practice and continuous improvement in line with legislation.To ensure that all staff in Digital and Security and across NSS have access to relevant information relating to information governance and are aware of their duties in relation to legal/policy/professional responsibilities for all aspects for Data Protection and Information Governance |

|  |  |
| --- | --- |
| **3. DIMENSIONS** |  |
| The post-holder will be based within the Information Security and Governance service area, providing support and expert advice to all staff in Digital and Security and across NSS. The job holder will have day to day responsibility for implementing NSS policy on data protection, privacy, information governance and related areas, supporting and developing policies and guidance for use in IT as appropriate. This will involve working collaboratively with the NSS Senior Consultant, Caldicott Guardians, and corporate leads in related information governance areas in other Strategic Business Units and boards when required to deputise for the Senior Consultant Information Governance. The post-holder has responsibility for the development and delivery of training on information governance and data protection matters across Digital and Security and the wider NSS.Customers include the Scottish Government, NHS Boards (and other NHS Organisations), other partner organisations (including those across the UK), the media, the public, commercial organisations and research bodies. |

|  |
| --- |
| **4. ORGANISATION CHART** |
|  |
|  |

|  |
| --- |
| **5. ROLE OF THE DEPARTMENT**  |
| Digital and Security (DaS)DaS operates as a centre of excellence for digital, security, governance, data and technology in Scotland, working collaboratively with public sector partners to identify and deliver trusted and secure digital solutions to help us all achieve the ambitions for health and social care in Scotland, while ensuring appropriate security, governance, compliance frameworks and policies are followed.DaS helps health boards to harness the transformative power of technology - making public services simpler, better and more efficient for the people who need them.Programmes vary from time to time but currently include Scottish Wide Area Network (SWAN), CHI (NHS Scotland’s national patient identifier infrastructure), NHSmail (our national email solution) and delivery of Microsoft Office 365 transformation programme, implementation of data breach detection solutions and various data protection compliance tools.**Information Security and Governance**Information Security and Governance (ISG), are a team working within the Digital and Security business unit delivering services including cyber security, governance and assurance, and advisory, delivery and security management of national contracts, and running a national NHS Scotland Security Operations Centre (SOC).The team also leads on delivering expertise and guidance on Information Governance strategies and frameworks including but not limited to Data Protection Legislation, as set and defined locally by the NSS DPO, Risk assessment and management and ensures alignment to Scottish Government policies, procedures and strategy including ‘Once for Scotland’ DaS staff are based primarily in Edinburgh and Glasgow.  |

|  |
| --- |
| **6. KEY RESULT AREAS** |
| 1. The post-holder will lead and implement all aspects of data protection, privacy, information sharing, information governance and related issues, ensuring appropriate policies and procedures are embedded. Devise and issue guidance to staff at all levels on privacy, information governance and data protection. The post-holder is required to interpret highly complex legislation and common law, analyse its impact on overall NSS policy and strategy, in order to apply appropriate and legal solutions across the whole organisation, often where there is no precedent on the way forward.
2. To provide leadership, liaison and support to managers, ensuring that the information governance implications of new technical and software developments are understood and that solutions are fit for purpose.
3. Using their knowledge of the relevant complex issues and legal requirements, and understanding of the potential obstacles that may emerge from current practice, the post-holder will contribute to the necessary policy developments that need to be adopted in relation to data protection, information governance and privacy, in order to help ensure legal compliance and safeguard stakeholder confidence. Contribute to the development of the annual business plan, ensuring all information governance objectives are clearly understood.
4. To maintain and continually update personal competencies and expert knowledgeof the field of data protection including privacy by monitoring current legislation on personal rights which affects the practices of handling personal data. Lead the planning, development and delivery of training programmes for all levels of staff, in response to legislative changes re data protection and information governance issues. Produce training materials and deliver training, to ensure staff understand and act upon any necessary changes to ways of working, which may be required to remain legally compliant.
5. Liaise with external stakeholder through active participation in programme boards and project teams, when required, ensuring that information governance considerations are understood and implemented.
6. Occasional phone and written correspondence with members of the public over concerns about privacy and data protection matters, including sensitive and contentious issues, and requests for access to their information. Ensuring that NSS Senior Consultant is kept informed of emerging issues.
7. Set up, maintain, contribute to project records, filing systems, websites, discussion groups and publish information on the local intranet and the external NSS website when required.
 |

|  |
| --- |
| **7. ASSIGNMENT AND REVIEW OF WORK and DECISIONS AND JUDGEMENTS** |
| The post-holder will establish his/her own detailed priorities and actions within a broad framework determined by the business objectives. The post-holder will adjust their priorities to meet frequently changing customer demands and will review these, self managing any conflicting demands, seeking advice from the NSS Senior Consultant only when necessary. Formal line management reporting for the post-holder will be to the NSS Senior Consultant on a monthly basis. If working out with Digital and Security, supervision may be assigned to the project sponsor. The post-holder may be required to work flexibly in short term project teams out with their usual service area, working with staff from other areas of Digital and Security to take forward short-life development projects.The post-holder will be working simultaneously across many issues and will be required to communicate in highly complex facts or situations which require the analysis, interpretation and comparison of a range of options, as well as legal and advisory sources, some of a complex and potentially conflicting nature. Conflicting demands occur frequently, which often require re-negotiation of existing deadlines with customers. |

|  |
| --- |
| **8. COMMUNICATIONS AND RELATIONSHIPS**  |
| **Internal*** Direct reporting on both an informal and formal basis to the Senior Consultant to update on key performance indicators, and the status of the Department.
* Direct liaison with senior managers and other department managers on IG requirements and issues associated with projects and activities across NSS.
* Direct contact on both an informal and formal basis with senior and business managers to understand and discuss current issues and ongoing initiatives.
* Attend Governance Groups, where appropriate.

**External*** Liaison with peers in the NHS Boards and other public sector bodies to maintain depth of knowledge in the specialist field.
* Review of external consultants and 3rd party service providers’ adherence to IG compliance
* Direct contact on both an informal and formal basis with senior and business managers within the NHSS and beyond to understand and discuss current issues and ongoing and future initiatives.
* Play a key IG specialist role across and number of National groups when deputising for the Senior Consultant, such as:
* NHSS / Atos IG / IT Security Group -ongoing liaison with Atos around policy and issue resolution
* National IG Leads Forum
* NSS Data Protection Leads Forum.
 |

|  |
| --- |
| **9. MOST CHALLENGING PARTS OF THE JOB** |
| * Keeping up-to-date with new and emerging technologies/legislation and policy in a rapidly developing environment. Ensuring the NSS is fully appraised of the merits and demerits of emerging technologies and that all developments are in line with NHS and NSS strategies.
* Applying expert specialist knowledge (in consultation with the Senior Consultant) across multiple complex projects to ensure system architecture and design is sufficiently robust and effective to meet the needs of business users across the NHS in compliance with Information Governance.
 |

|  |
| --- |
| **10. SYSTEMS** |
| The post holder is jointly accountable for the information governance and data protection compliance of major IT systems across the stakeholder base and also for approved standards and policy compliance. Services are delivered to NSS, NHS Scotland NHS Boards, Hospitals, Primary Care Practitioners, Community Health Partnerships, Local Authorities, Scottish Government Directorates, other UK eHealth agencies, and major product and service providers operating in the Scottish public sector.The post-holder will make use of computer technology on a daily basis for routine office work, generating reports, producing NSS guidance documentation, and will also use e-mail, intranet and internet for information, research and communication purposes.The post-holder will maintain accurate up to date office files both paper and electronic and supervise website content and make recommendations for re-design where necessary. The post-holder will be expected to understand and analyse eHealth and other solutions for Data Protection threats and opportunities. The post-holder will make use of national and local office technologies such as eEss, eExpenses and the Crown flexi-time system.  |

|  |
| --- |
| **11. PHYSICAL, MENTAL, EMOTIONAL EFFORT** |
| **Physical effort**Light to moderate: includes moving light equipment e.g. briefcases/lap-tops, projectors for presentations; using keyboards frequently for word-processing, spreadsheets etc and e-mail. **Mental effort**Intense concentration/ in-depth mental attention frequently required e.g. leading meetings, influencing Scottish Government and NHS staff and managers at all levels of seniority, public speaking, analysing technical and other system problems and proposing solutions; often working under pressure and balancing multiple demands in complex/ changing environments.**Emotional effort**Exposure to occasional distressing circumstances, in particular when dealing with members of the public as an NSS official. Involves from time to time dealing with conflict situations e.g. in emotionally charged meetings. Dealing regularly with challenging problems requires sustained emotional energy/ resilience.  |

|  |
| --- |
| **12. ENVIRONMENTAL/WORKING CONDITIONS & MACHINERY AND EQUIPMENT** |
| Standard office conditions. Ongoing use VDU.Standard keyboard skills.Regular travel which can be for extended periods of time.  |

|  |
| --- |
| **13. KNOWLEDGE, TRAINING AND EXPERIENCE REQUIRED TO DO THE JOB** |
| Highly developed specialist knowledge across the range of work procedures and practices involved in information governance and data protection, underpinned by theoretical and legal knowledge and relevant practical experience.Experience of working at a senior level in the information governance field. The post holder will have excellent communication and interpersonal skills and will have the ability to effectively lead and motivate people. The ability to liaise effectively with senior internal NHS managers and senior external managers is essential. Proven customer facing skills and the ability to work well under pressure are also essential qualities for the post.Policy development and project management skills. Knowledge of the structure and delivery of NHS healthcare services is desirable.  |
|  |
| **14. JOB DESCRIPTION AGREEMENT** |
| A separate job description will need to be signed off by each postholder to whom the job description applies. |
| Postholder Signature: |  | Date: |  |  |
|  |  |  |  |  |
| Postholder Print: |  |  |  |  |
|  |  |  |  |  |
| Manager Signature: |  | Date: |  |  |
|  |  |  |  |  |
| Manager Print: |  |  |
|  |  |  |  |  |
| Manager Title: |  |  |
|  |  |  |  |  |
|  |  |  |  |  |