SINGLE CORPORATE SERVICES

DIGITAL SERVICES

Job title:	Security Architect	
Reporting to:	Head of Technical Delivery	
Accountable to:	Associate Director of IT	
Pay Band:	8A	

As part of the Single Corporate Service, this role provides a service across both Isle of Wight NHS Trust and Portsmouth Hospitals University NHS Trust.

The intention for the existing primary work locations to remain unchanged as there is no desire to change base locations unnecessarily. However, as the single corporate service will be delivered across both organisations, individuals may be required to undertake business travel from time to time. The staff mobility local agreement will apply.

For our leaders managing staff across multi-site locations, they will need to be visible and provide in person leadership. The arrangements and frequency will be agreed locally.

The OneEpr Programme exists to implement a single integrated electronic patient record (EPR) designed to improve patient outcomes and the experience of delivering care for our colleagues.

The solution is the direct result of the combined vision and strategic goals of:

1. Isle of Wight NHS Trust (IWT)
2. Portsmouth Hospitals University NHS Trust (PHU)
3. Hampshire Hospitals NHS Foundation Trust (HHFT)
4. University Hospital Southampton Foundation Trust (UHS)

The Trusts will work together with their clinical and departmental experts alongside regional digital colleagues to procure and implement a joint EPR over the coming years .

The introduction of EPR will support us in transforming how we work every day, helping us to run our services with the information we need at our fingertips. It will also help us to deliver care in a different way, according to best practice, efficiently and consistently.

Our EPR will act as an enabler for a greatly improved integrated healthcare system, in which caregivers and patients have electronic access to more complete health records and are empowered to make better health decisions. The key objectives of the programme are:

1. Enhance patient care by empowering clinicians, providing them with the right information at the right time and in the right place
2. Improved continuity of care for many of our patients who receive treatment at more than one Trust
3. Provide a ‘single source of truth’, making sharing information across pathways much simpler

4. Maximise efficient working and reduce errors when making decisions
5. Allow significantly greater clinical information-sharing with our partners in primary care, community care, mental health and ambulance
6. Enable integration of acute services across the four Trusts

Job purpose

This is a leading senior technical role within the Cyber Security team with accountability for the definition of the security solutions and architecture for applications, information and infrastructure in transforming the underlying IT supporting the business

The role will be responsible for secure IT solutions as the the trust transforms the way it provides services; maximising their availability, integrity and security for end-users and optimise the value gained by the Trust from its investment in IT.

The post holder will work with trust business areas to understand and shape their security requirements, ensuring that patient data and other assets are secured, whilst enabling open and modern secure digital services. You and will be accountable for the control of the IT Security technical design documents which define the end state architecture for the trust.

Responsibilities includes providing security advice and key constraints to trust technology & business teams team in ensuring project deliveries remain aligned to the defined risk appetite. You will be actively involved in defining secure solutions for the trust.

Play a leading senior technical role in the provision of effective, efficient and fully integrated ICT operational services that maximise their availability, integrity and security for end-users and optimise the value gained by the Trust from its investment in ICT. This will be achieved by;

- Designing, building and overseeing the implementation of network and computer security with varying complexities ensuring business strategies and processes are considered in translation to IT solutions;
- Ability to operate across organisation and computer technology 'silos' to drive common security approaches across the Trust enterprise architecture;
- Acting as champion for the department's Security processes, establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Information Security Management System (ISMS).
- Provide leadership in securing the enterprise architecture technologies when working with external vendors, suppliers and other stakeholders.
- Using Risk assessment procedures recommend and document security controls and identify solutions that support a business objective
- As a senior-level employee, you'll be responsible for creating complex security structures – and ensuring they work.
- Acting as the IT Security champion for any external or internal security audits & penetration checks. Leading on the remediation plans and securing the required funding as required.

Job summary

- Proactively and positively contribute to the achievement of deliverables through individual and team effort. Manage the production of the required deliverables and control risks,
- Support team members to deliver on their functionally relevant objectives through offering

advice, guidance and support as appropriate.
- Ensure that approved budgets are spent effectively and in accordance with agreed procedures
- Liaison with Senior Professionals and related functions to ensure that work is neither overlooked nor duplicated
- Build and sustain effective communications with other roles involved in the shared services as required
- Maintain and continuously improve specialist knowledge in an aspect of Health Service which significantly contributes to the Trust's stated objectives & aims
- Establish and maintain strategic links with a range of external partners/stakeholders or manage the links made through the team. Engage with external partners/stakeholders to gain their necessary level of contribution & commitment to the successful delivery of your work.
- Undertake proactive horizon scanning for either developments relating to Trust work or opportunities for Trust involvement around health issues
- Increase the level of knowledge & skills within the Trust through documenting key learning and supporting others to develop their professional abilities.
- Dissemination of knowledge through engagement in report writing, and reviewing, taking full responsibility for technical accuracy and reliability and being sensitive to the wider implications of that dissemination.
- Ensure that expertise is seen as a resource within and outside the Trust and form working partnerships with government departments, national agencies and key stakeholders.
- Develop structures, systems, ways of working and personal values that will support the Trusts sustainable development objectives with regard to issues such as Carbon reduction and waste minimisation; and to encourage all stakeholders of the Trust to act as enthusiastic agents of change.

Specific Core Functions

- Acquire a complete understanding of the trusts enterprise architecture including, business processes, technology and information systems
- Responsible for the technology security standards, lead engineer for security technology platforms and tools
- Plan, research and design security architectures for both technical and business led projects
- Perform vulnerability testing, risk analyses and security assessments
- Research security standards, security systems and authentication protocols
- Review and approve installation of firewall, VPN, IDS and NAC policies and devices
- Define, implement and maintain trust security polices and procedures
- Respond immediately to security-related incidents and provide a thorough post-event analysis
- Act as a champion of knowledge and skills in security specific areas of technologies, sharing these skills and knowledge with colleagues within the department. Develop staff so they have the ability to better understand how the Security architecture and IT components interact with each other

Key Responsibilities

Communication and Working Relationships

- Build and sustain effective communications with other roles involved in the shared services as required
- Build and sustain effective communications with other Trust functions and positions involved with digital and transformation agenda as appropriate.
- Provide leadership and advice to Board, Executives, clinicians and managers on all aspects of Digital infrastructure.

- As a senior specialist be involved in meetings, feedback sessions etc. where highly complex, sensitive, emotive and sometimes highly contentious information is conveyed.
- Facilitate, train and advise on the appropriate and proportionate investigation/review of service development and sustainability
- Develop and maintain effective relationships and operational links with staff at all levels and disciplines, persuading and influencing engagement, and ensuring that risks, safety and quality issues; audit and other assurance sources, both inform and translate into positive service Business Partner improvements.
- Ensure complex, highly sensitive or contentious information is communicated clearly, appropriately and effectively to the target audience, ensuring that reasons and rationale are fully understood. Through this process to work with staff, at all levels, to obtain cooperation, to promote alternate ways of working, to negotiate solutions and to ensure ownership and implementation of positive changes and understand areas for improvement
- To discuss sensitive and contentious information with staff from all levels of seniority using negotiating, persuasive and empathetic skills, for example during a complex and extensive incident whereby conflicting points of view maybe expressed.
- To be responsible for overseeing the Digital processes, providing leadership and support.
- Actively encouraging positive discussion to alleviate concerns and resolve issues.
- Demonstrate a high level of written and verbal communication skills, conveying complex information

Analytical and Judgement

- Maintain and continuously improve specialist knowledge in an aspect of Health Service which significantly contributes to the Trust's stated objectives & aims
- Establish and maintain strategic links with a range of external partners/stakeholders or manage the links made through the team. Engage with external partners/stakeholders to gain their necessary level of contribution & commitment to the successful delivery of your work.
- Undertake proactive horizon scanning for either developments relating to Trust work or opportunities for Trust involvement around health issues
- Increase the level of knowledge & skills within the Trust through documenting key learning and supporting others to develop their professional abilities.
- Dissemination of knowledge through engagement in report writing, and reviewing, taking full responsibility for technical accuracy and reliability and being sensitive to the wider implications of that dissemination.
- Ensure that expertise is seen as a resource within and outside the Trust and form working partnerships with government departments, national agencies and key stakeholders.
- As lead expert and specialist ensure that excellent judgement skills are used when considering options available in relation to Digital services.
- Ability to interpret, analyse and translate a wide range of managerial information to underpin evidence based decision making.
- Analyse data so that trending can be discussed at management groups, quality governance and performance meetings.
- To analyse information and ensure action is taken to improve services.
- To be responsible for analysing data. This data will often be multi-faceted and complicated in nature.
- Encourage a learning culture to ensure continuous improvement, and organisational learning from concerns and assurance processes including audit.
- To plan, facilitate and implement change projects to implement the Trust's revised policies and strategies, ensuring that resources are identified appropriately to enable staff and the service to develop.

- Develop the required level of information to be reported to the Board and any nominated committee, sub-committee or group.
- Support the trust, including through the provision of training on a wide range of Digital subjects, to understand and own the integrated governance and quality agenda and associated policies and strategies to ensure its efficient and effective operation and accountability.
- The post holder will be required to develop and project manage their own projects and supervise work on relevant and related projects.
- Provide specialist advice on Digital governance issues to both clinical and non-clinical staff. On occasion the post-holder may be required to provide such advice to service users and their relatives.
- Lead on improving the management of Digital services and learning across the Trust, developing, testing and leading improvements, working closely with appropriate service leads.
- Skills to innovate solutions that provide value both in terms of defensive/protective measures and reduce the time to detect and contain attacks
- Skills to align business and security objectives and speak the cost-benefit language, especially as it gets easier, cheaper and faster to deploy cloud-based solutions
- Skills to integrate the tool sets to better manage the threats, vulnerable systems and ultimately know what to protect and how.
- Sets security policies and influences IT Users in defining their needs for new access rights and privileges.
- Provides professional advice for enquires related to clinical information and personal information security.
- Provides professional technology subject matter expertise advice to the department's business contingency planning.

Planning and organising

- The post holder organises own day-to-day work tasks or activities.
- Support the Digital senior leaders in provision of routine and ad-hoc reports, plans and risks to Trust Board, Trust Leadership Team, Digital Committee and other bodies to ensure digital issues are understood and responded to in an appropriate manner at all levels of the organisation.
- Represent the Digital Department at local levels, developing partnerships, sharing best practice and integrating knowledge within the Trust.
- Review existing strategies for the achievement of CQC standards and develop new strategies as required.
- Conduct gap analyses against existing and any new standards/best practice guidance or assessment processes to ensure the trust constantly seeks to improve its position.
- Work towards embedding the culture of continuous improvement across the services, ensuring that departments take ownership across all staff groups
- Be pivotal in reinforcing the importance of proactive management, assurance and governance as an underpinning means of ensuring quality, promoting a multidisciplinary approach to improvement and ultimately patient safety
- To identify training needs through implementation of the service and quality agenda.
- Work in conjunction with the team to deliver effective programmes of education and training, taking an active role in teaching on these programmes and any initiatives as appropriate.

Physical Skills

- Ensure own continuing professional development, maintaining specialist and managerial credibility.
- Be able to travel across to different sites and various community settings where required.
- Proficient in the use of information technology and keyboard skills, able to produce high quality reports.

Patient Client Care

- Any patient contact will be incidental

Policy and Service Development

- As an influential member within the Digital Department share collective responsibility for setting departmental policy, agreeing workload priorities and resolving internal issues to ensure the whole Department supports and enhances Trust service delivery to patients and the very best of its ability.
- Contribute to the development and implementation of long-term corporate digital strategies.
- As lead specialist develop, monitor, implement and ensure timely review of policies and procedures throughout the Trust.
- Design, develop and implement policies and processes to ensure that the Trust meets its legislative and CQC requirements.
- Working with divisions to ensure that changes are made, and/or systems and services are developed.
- Contribute to the development of a robust framework and strategy that fosters a culture of ownership, inclusion and accountability, whilst encouraging innovations and problem solving.
- Identify and implement key projects and effective systems to monitor compliance within governance requirements.
- To participate in reviewing policies, updating and disseminating them as required.
- To participate in meetings across the divisions.
- To drive divisions services in line with ongoing national agenda and local Trust initiatives.
- To work with other Departments and divisions to support the achievement of overall Trust objectives.
- To complete ad hoc tasks and projects as requested

Financial Management

- The post holder holds a delegated budget from a budget for a department/service.

Management/Leadership

- Support team members to deliver on their functionally relevant objectives through offering advice, guidance and support as appropriate.
- Liaison with Senior Professionals and related functions to ensure that work is neither overlooked nor duplicated
- Support Digital senior leaders to ensure a cohesive, coordinated approach to all aspects of delivery enabling the Department, as a whole, to meet priority demands and ensure needs of the Trust and Department supersede those of individual services and staff.
- Support Digital senior leaders to ensure robust processes are implemented to maintain Departmental compliance with information governance, cyber security, Freedom of

Information, data protection, Caldicott, health & safety, major incident planning, risk management, equality & diversity and other relevant requirements.

- Take a shared responsibility for overall performance of the Department and timely delivery of its targets and objectives.
- To undertake the full range of Human Resource procedures involved with managing or supervising staff within the team as may be required.
- Have a working knowledge of Trust policies.
- Lead by example, actively presenting as a role model in own behaviour and fostering an inclusive culture.
- Actively promote change, improvement and knowledge sharing.
- Promote a safe environment for exchange of views and ideas.

Information Resources

- Lead responsibility for ensuring active maintenance of data bases to ensure accuracy of performance reporting to the Trust Board, Committees, commissioners and NHS England; ensuring that the quality of information is up to date so as to enable detailed trend analysis and theming to be undertaken
- To be familiar with the use of the Ulysses so that the post- holder is proficient in eliciting and interpreting information for analysis purposes.
- Accurately record personally generated information, maintaining records in accordance with Trust policies and procedures, the Data Protection Act and Caldicott principles at all times.
- Maintain accurate statistical information and data using databases as necessary to inform and drive programme of work.
- Enable assurance through analysis of data captured through metrics, research projects, service improvement initiatives and audit, and actively encourage the use of information to improve the quality of services
- Collate as required, qualitative and quantitative information and lead appropriate analysis to develop business cases and contribute to project 'products'.
- Initiates the software builds ready for loading onto the target hardware. Held within a configuration management standard arrangement, conducts a series of tests and records the details of any failures.
- Produces test specifications as required for testers to follow, carries out fault diagnosis relating to extreme complex problems as part of installations, reporting the results of the diagnosis in a clear and concise manner.
- Installs or removes hardware and/or software, using installation instructions and tools, follows agreed standards.
- Adheres to the IT Change and Release Management Process for all software and hardware changes.
- Reports details of all hardware/software items that have been installed and removed so that configuration management records can be updated.
- Contributes, as required, to the development of installation procedures and standards
- Working alone or leading a project team on highly complex IT systems and modifications to existing IT systems, or with partners, vendors or colleagues on complex enterprise systems.
- Specifies user/system technical requirements, including the overall management of the system implementation and transition into both the Operational Service and Centre.
- Designs and completes detailed analysis of systems/infrastructure which meets security standards and are resilient in the event of disaster.
- Designs and executes test plans, to verify correct operation of completed system implementations.

- Documents all work using required standards, methods and tools, including internal tools where appropriate.
- Prepares and maintains operational documentation for relevant system software within the Trust Data Centre. Advises other IT staff on the correct and effect use of system software.
- Collects performance data to monitor system efficiencies against either published service level agreements or vender best practice thresholds. Monitors both resource usage and failure rates of installed systems and provides feedback to IT Operations Management Team.
- Gathers performance statistics from the hosted IT Systems to enable recommendations for the tuning of System Infrastructure. Initiate system software parameters to maximize throughput and efficiencies
- Provide guidance, coaching and collaborative working with Technical Architects to provide consensus based enterprise solutions that are scalable, adaptable and in synchronization with ever changing business needs.
- Leading role in regular discussions regarding internal process and system improvements in order to ensure maximum efficiency across the organisation and enterprise architecture. Including suggesting varying complexities of technical solutions to on going and potential problems.
- Alignment of IT strategy and planning with Trusts business goals by leading planning sessions with Trust business decision makers.
- Lead on multi vendor architecture strategies and major incident resolution situations. Acting as subject matter expert of multiple enterprise technologies ensuring the Trust benefits from It solutions.
- Form part of the IT departments Design Authority and contribute to the long-term strategy for the Trusts IT core architecture.
- Promotion of shared infrastructure and applications to reduce costs and maximise the benefits from server and storage virtualised technologies. Ensure that projects do not duplicate functionality or diverge from each other and business and IT strategies.
- Direct or indirect involvement in the development of policies, standards and guidelines that direct the selection, development, implementation and use of Information Technology within the enterprise.
- Act as a champion of knowledge and skills in specific areas of technologies, sharing these skills and knowledge with colleagues within the department. Develop staff so they have the ability to better understand how the IT components interact with each other.

Research and development

- Regularly undertakes R&D activity as a requirement of the job, or regularly undertakes clinical trials, or regularly undertakes equipment testing or adaptation.
- Analyse relevant data and evidence based findings to inform own work programme, and to design and introduce new initiatives relevant to agreed objectives.
- Horizon-scan for newly published research and studies, use advanced critical analysis skills to assess the validity of findings, and where appropriate, strategically lead work to implement as part of agreed work objectives

Freedom to Act

- Proactively and positively contribute to the achievement of deliverables through individual and team effort. Manage the production of the required deliverables and control risks
- Nurture strong and positive working relationships with Divisions, to ensure digital expectations are managed and met through a shared understanding of Division and Digital Department needs, issues, priorities and capabilities.

- Using a high level of sensitivity and diplomacy, manage expectations when new business ideas prove unworkable, do not fit strategically or do not provide value for money (identifying alternative solutions where possible).
- Act as 'champion' for Divisional and clinical needs within the Digital Department. Provide perspective that helps to educate Digital colleagues in Trust and healthcare operations and processes that ensures requirements are appropriately understood and safe, patient-centric user friendly solutions and services are provided.
- Coach Divisions in planning, scoping, implementing and using digital services & solutions to deliver productivity & efficiency gains and raise digital maturity across the Trust. Ensure that Digital considerations are included in prior approval and formal procurement, financial procedures are complied with and project management processes are followed for implementation.
- Identify key areas in which digital services & solutions can transform or streamline functions and tasks. Analysing and interpreting highly complex facts & situations and comparing ranges of options; support Divisions in development of digital business plans and business cases and; provide the link to the Digital Department to ensure that the right expertise and resource is connected at the right time.
- Carry out initial reviews of Divisional digital proposals to determine feasibility and avoid duplication. Manage expectations where proposals do not demonstrate strategic fit, provide adequate benefit realisation or are unworkable.
- Ensure all Divisional information systems, services and contracts comply with requirements of Trust information security/governance and procurement policies & procedures and benchmarked against best practice. Identify gaps in practice and highlight these to responsible managers with recommendations on how they should address them.
- On behalf of the Digital Department, act as the first point of contact for Divisions, focusing on customer issues and priorities, performance against SLA targets and raising of digital developments and issues. Establish escalation processes to ensure key issues are addressed appropriately.
- As an expert, develop and implement a long-term strategic approach for the introduction and maintenance of systems which recognise the need to learn from concerns, incidents and assurances, as well as seeking effective resolution for services
- Interpret national guidance and legislation to determine its applicability to the Trust, working with other divisions leadership teams to take any actions required to improve adherence.
- Accountable for own work programme, and is required to provide advice and guidance to Trust staff in relation to all aspects of the agreed work programme.
- Required to exercise specialist knowledge across a range of procedures and practices underpinned by theoretical knowledge and practical experience
- Responsible for day to day operational management and strategic development associated with agreed objectives.
- Work with minimal supervision. This will require balancing the need for proactive service development and strategic leadership against reactive demands.
- Lead the development, planning and implementation of a broad range of complex activities, taking action as needed to ensure successful delivery of agreed outcomes, reporting progress and working across the central team to inform strategy and organisational learning.
- Exercise own judgement based on interpretation of highly complex facts to inform own work priorities.
- Influence and negotiate with stakeholders across all levels of the organisation to progress the agreed work programme.
- Make recommendations, provide advice and prepare strategic reports/briefings for the trusts leadership teams and others as required.

Physical effort

- There is a frequent requirement for sitting or standing in a restricted position for a substantial proportion of the working time,

Mental effort

- There is a frequent requirement for concentration where the work pattern is predictable with few competing demands for attention, or there is an occasional requirement for concentration where the work pattern is unpredictable.

Emotional Effort

- Exposure to distressing or emotional circumstances is rare, or occasional indirect exposure to distressing or emotional circumstances.

Working conditions

- Requirement to use Visual Display Unit equipment more or less continuously on most days.

Person Specification

Criteria	Essential	Desirable	*How criteria will be assessed*
Qualifications	• Degree level qualification or equivalent in computer science, Cyber security or a related field • Technical accreditation in at least two or more of the following; Microsoft Certified Systems Engineer (MCSE) Cisco Certified Network Associate Security (CCNA Security), VMware VCP • ITIL Foundation Certificate • Evidence of continuing professional development	• ITIL Practitioner qualification • CISSP: Certified Information Systems Security Professional • CISSP-ISSAP: Information Systems Security Architecture Professional • CISM: Certified Information Security Manager • CEH: Certified Ethical Hacker • CSSA: Certified SCADA Security Architect • CCP: CESG Certified Professional • Cisco Cybersecurity specialist (SCYBER) • Cisco Certified Network Professional Security (CCNP Security) • Cisco Certified Internetwork Expert	**Application and Interview**

		Security (CCIE Security) • Enterprise architecture frameworks such as TOGAF, SABSA. • Checkpoint (CCSA, CCSE, CCMSE, CCSM) • BCS Practitioner in Information Assurance Architecture • GIAC Global Information Assurance Certifications	
Experience	• Advanced theoretical and enterprise knowledge across three or more information technology platforms: Server Virtualisation, Desktop Virtualisation, Data & Voice Networking, Messaging, Storage Area Networks, Security, Mobility, Server & Peripheral Hardware. • Advanced theoretical and enterprise knowledge across Network Data & Infrastructure Security • Significant experience of pragmatic Security risk assessments through frameworks of security controls and security management strategies • Significant experience of IT Service Management, Incident Management, Problem Management, Change Management, Performance Management & Availability Management. • Significant experience of Security Architecture Design	• At least 3-5 years of relevant IT experience devoted specifically to security • Knowledge and understanding of the HSCIC Information Governance guidance, including but not limited to:- o Confidentiality – Standards of practice for health record confidentiality o IG Toolkit – IC standards and guidance for NHS and partner organisations o Information Security – Safeguards and guidelines for protecting patient data o NHS Codes of Practise and legal obligations o Information Governance Alliance (IGA) o National Data Guardian (NDG)	**Application and Interview**

	• Significant experience in leading highly complex technical and security problems to resolution, including team management and managing external suppliers. • Significant experience in leading project delivery of technical projects. • Experience in assisting with report writing, being operating procedures, options appraisals, Security policy writing, risk analysis, user guides. • At least 5-10 years of relevant IT experience, including exposure to business planning, systems analysis and application development		
Knowledge	• Excellent interpersonal and explanatory skills in dealing with a wide range of information technology users from skilled to ICT-illiterate. • Excellent verbal/written communication skills, with the ability to present within a group. • Good team-player, highly motivated individual to support the delivery of an efficient, effective customer-focused support service. • Good presentation and negotiation skills to produce and present formal proposals and get proposals accepted.	• Security monitoring detection and response software • Knowledge of the following technical skills would be desirable: • Risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies and security attack pathologies. • ISO 27001/27002 • Microsoft Windows, UNIX and Linux operating systems • Perimeter security controls – Firewall	**Application and Interview**

	• Excellent planning and time-management skills. • Good negotiating and relationship-building skills to gain maximum benefit for customers from software suppliers and internal ICT providers. • Able to set clear and appropriate priorities, with the ability to deal with conflicting demands, unpredictable work patterns, and multiple deadlines. • Good technical knowledge to understand and resolve enterprise technical problems. • Excellent knowledge of data protection and information security/governance issues. • Good knowledge of providing proactive IT System/Network performance monitoring.	(Checkpoint preferable), IDS/IPS, Network access controls and network segmentation • Router, Switch and VLAN security; wireless security • Security concepts relating to DNS, routing, authentication, VPN, proxy services and DDOS mitigation • Monitor, proactively analyse traffic for security threats and mitigate identified security incidents that have emerged	

Compliance statement to expected organisational standards.

To comply with all Trust Policies and Procedure, with particular regard to

- Risk Management
- Health and Safety
- Confidentiality
- Data Quality
- Freedom of Information
- Equality Diversity and Inclusion
- Promoting Dignity at Work by raising concerns about bullying and harassment
- Information and Security Management and Information Governance
- Counter Fraud and Bribery

The Trust has designated the prevention and control of healthcare associated infection (HCAI) as a core patient safety issue. As part of the duty of care to patients, all staff are expected to: Understand duty to adhere to policies and protocols applicable to infection prevention and control.

- Comply with key clinical care policies and protocols for prevention and control of infection at all time; this includes compliance with Trust policies for hand hygiene, standards (universal) infection precautions and safe handling and disposal of sharps.
- All staff should be aware of the Trust's Infection Control policies and other key clinical policies relevant to their work and how to access them.
- All staff will be expected to attend prevention and infection control training, teaching and updates (induction and mandatory teacher) as appropriate for their area of work, and be able to provide evidence of this at appraisal.

- To perform your duties to the highest standard with particular regard to effective and efficient use of resources, maintaining quality and contributing to improvements.

- Ensure you work towards the Knowledge and Skills Framework (KSF) requirements of this post. KSF is a competency framework that describes the knowledge and skills necessary for the post in order to deliver a quality service.

- Your behaviour will demonstrate the values and vision of the Trust by showing you care for others, that you act professionally as part of a team and that you will continually seek to innovate and improve. Our vision, values and behaviours have been designed to ensure that everyone is clear about expected behaviours and desired ways of working in addition to the professional and clinical requirements of their roles.

- Ensure you adhere to and work within local and national safeguarding children legislation and policies including the Children Act 1989 & 2004 , Working Together to Safeguard Children 2013, 4LSCB guidance and the IOW Safeguarding Policy.

- Ensure you adhere to and work within the local Multiagency safeguarding vulnerable adults policies and procedures

- Ensure that you comply with the Mental Capacity Act and its Code of Practice when working with adults who may be unable to make decisions for themselves,

- Ensure that you maintain personal and professional development to meet the changing demands of the job, participate in appropriate training activities and encourage and support staff development and training.
- Respect the confidentiality of all matters that they may learn relating to their employment and other members of staff. All staff are expected to respect conform to the requirements of the Data Protection Act 1998, including the responsibility to ensure that personal data is accurate and kept up to date

- If your employment is to a post that requires you to be registered with a professional body, the continuation of your employment is conditional upon you continuing to be registered with the appropriate professional body. The Trust will require evidence of current registration.

- Proactively, meaningfully and consistently demonstrate the Trust Values in your every day practice, decision making and interactions with patients and colleagues.

- Perform any other duties that may be required from time to time.

- Contribute to the IT Departments on-call rota and if required, maintain required skills, experience and resource levels allowing for hospital digital 24/7 services.

This job description may be altered, from time to time, to meet changing needs of the service, and will be reviewed in consultation with the post holder.