

29th September 2026

Eastbourne District General Hospital

Kings Drive
Eastbourne
East Sussex
BN21 2UD

Tel: 0300 131 4500
Website: www.esht.nhs.uk

Further to your recent request for information made under the Freedom of Information Act (FOIA) 2000, I now set out our answers to your specific questions, and any clarifications sought and provided, as follows:

Please provide the following information:

- 1. Is the Trust's IT service desk/helpdesk managed by the Trust's internal team/s or outsourced in whole or part?**

East Sussex Healthcare NHS Trust's IT service desk/helpdesk is managed by ESHT's internal teams.

- 2. What, if any, elements of the IT service desk/helpdesk and clinical system management are provided through an external managed service provider or external resource?**

None.

- 3. Please provide details of any current organisational charts, governance documents, operating models, or role descriptions relating to the Trust's IT service desk/helpdesk, including the use of internal staff, contractors, temporary resource augmentation, or managed service providers**

Please see attached the following documents:

- [24-240 JD Service Desk Analyst B4_Redacted](#)
- [Digital Delivery 120226_Redacted](#)
- [IT Operations Manager ESHT Digital_Redacted](#)
- [374-LVBDA071_Service Desk Manager - job description and person specification_Redacted](#)

Please note that it is the Trust's FOI policy to only provide the names of staff that are graded at Band 8a (senior staff) or above, and therefore the names of staff at Band 7 and below have been redacted from the attached documents.

Please also note we are applying Sections 31(1)(a) and 40(2) as we have redacted the names of the Trust's IT Systems and staff that no longer work for the Trust, as set out below:

Section 31(1)(a)

Under Section 31(1)(a) of the Freedom of Information Act (FOIA), the Trust can confirm that it holds information relevant to your request, however, we are unable to disclose it for the reasons explained below.

Historically, we would disclose information relevant to the Trust's IT systems, infrastructure and software as part of our transparency agenda under the terms of the Freedom of Information Act (FOIA). However, in light of the recent cyber-attacks on NHS hospitals and the serious impact these have had on patient services and the loss of patient data, we are having to reconsider this approach. Please see several links to news articles about these recent cyber incidents provided below for your information.

- [*NHS England — London » Synnovis Ransomware Cyber-Attack*](#)
- [*NHS England confirm patient data stolen in cyber attack - BBC News*](#)
- [*Merseyside: Three more hospitals hit by cyber attack - BBC News*](#)

As a result of these attacks, thousands of hospital and GP appointments were disrupted, operations were cancelled, and confidential patient data was stolen which included patient names, dates of birth, NHS numbers and descriptions of blood tests.

When we respond to a Freedom of Information request, we are unable to establish the intent behind the request. Disclosure under the FOIA involves the release of information to the world at large, free from any duty of confidence. Providing information about our systems or security measures to one person is the same as publishing it for everyone. While most people are honest and have no intention of misusing information to cause damage, there are criminals who look for opportunities to exploit system weaknesses for financial gain or to cause disruption.

In the context of the FOIA, the term "public interest" does not refer to the private or commercial interests of a requestor; its meaning is for the "public good". The Trust receives a significant number of requests each year regarding our IT systems, infrastructure and cyber security measures. Most of these requests are commercially driven and serve no direct public interest. Information relevant to our IT portfolio is often requested by consultancy companies who then pass on this information to their client base. Many of these requests are submitted through the FOI portal [whatdotheyknow.com](#) who publish our responses, making this information available to an even wider audience.

As a large NHS Trust we hold extensive personal data relevant to our patients and staff, much of which is considered very sensitive. A lot of this information is held electronically on various administration and clinical systems. We have a duty under the Data Protection Act 2018 and the UK GDPR to protect this personal information and take all necessary steps to ensure this data is kept safe. This means not disclosing information that could allow criminals to gain unlawful access to our systems and infrastructure. The Trust can be heavily fined should it be found to have acted in a negligent way which

results in a personal data breach. We need to demonstrate that we comply with our legal obligations under data protection and freedom of information legislation, but we must be careful that too much transparency does not result in harm to our patients or staff, or cause disruption to our services.

Moreover, under the Network and Information Systems (NIS) Regulations Act 2018, operators of essential services such as NHS organisations like ours have a legal obligation to protect the security of our networks and information systems in order to safeguard our essential services. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in Section 10 of the Network and Information Systems Regulations 2018. Should we not comply with these requirements regulatory action can be taken against the Trust. Further information about the Network and Information Systems (NIS) Regulations Act 2018 can be found here – [The Network and Information Systems Regulations 2018: guide for the health sector in England - GOV.UK](#)

Your request asks for policy documents which unfortunately mention specific details regarding our IT Systems which, for the reasons explained above, would be inappropriate to release into the public domain. If disclosed, it is possible that patient data as well as other confidential information would be put at risk. Such disclosure could also impact on the security of our systems and result in serious disruption to the health services we deliver to the local community. Section 31(1)(a) of FOIA provides that information is exempt if its disclosure would, or would be likely to, prejudice (a) the prevention or detection of crime. In this case, disclosure would be likely to prejudice the prevention of crime by enabling or encouraging malicious acts which could compromise the Trust's IT systems and infrastructure. The Trust's capacity to defend itself from such acts relates to the purposes of crime prevention and therefore Section 31(a) exemption is applicable in these circumstances. For these reasons, the Trust considers disclosure of the information you are seeking to be exempt under Section 31(1)(a) [law enforcement] of the FOIA and the names of the IT systems within the policy is being withheld. The full wording of Section 31 can be found here: [Freedom of Information Act 2000](#)

Section 31 is a qualified exemption and therefore we must consider the prejudice or harm that may be caused by disclosure of the information you have requested, as well as apply a public interest test that weighs up the factors in maintaining the exemption against those in favour of disclosure.

In considering the prejudice or harm that disclosure may cause, as explained should the Trust release information into the public domain which draws attention to any weaknesses relevant to the security of our systems or those of a supplier, this information could be exploited by individuals with criminal intent. Increasing the likelihood of criminal activity in this way would be irresponsible and could encourage malicious acts which could compromise our IT systems or infrastructure, result in the loss of personal data and/or impact on the delivery of our patient services. We consider these concerns particularly relevant and valid considering the increasing number of cyber incidents affecting NHS systems in recent years and the view by government, the ICO and NHS leaders that the threat of cyber incidents to the public sector is real and increasing.

- [*Organisations must do more to combat the growing threat of cyber attacks | ICO*](#)

In the Government's Cyber Security Strategy 2022-2030, the Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office states on page 7:

“Government organisations - and the functions and services they deliver - are the cornerstone of our society. It is their significance, however, that makes them an attractive target for an ever-expanding army of adversaries, often with the kind of powerful cyber capabilities which, not so long ago, would have been the sole preserve of nation states. Whether in the pursuit of government data for strategic advantage or in seeking the disruption of public services for financial or political gain, the threat faced by government is very real and present.

Government organisations are routinely and relentlessly targeted: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating.”

With this in mind, we then considered the public interest test for and against disclosure. It should be noted that the public interest in this context refers to the public good, not what is 'of interest' to the public or the private or commercial interests of the requester. In this case we consider the public interest factors in favour of disclosure are:

- Evidences the Trust's transparency and accountability
- Provides information relevant to the IT systems and applications the Trust uses
- Reassures the public and partners that the Trust procures these systems in line with Procurement legislation
- Reassures the public and partners that the Trust's IT infrastructure and systems are secure

Factors in favour of withholding this information are:

- Public interest in crime prevention
- Public interest in avoiding disruption to our health services
- Public interest in maintaining the integrity and security of the Trust's systems
- Public interest in the Trust avoiding the costs associated with any malicious acts (e.g. recovery, revenue, regulatory fines)
- Public interest in complying with our legal obligations to safeguard the sensitive confidential information we hold

In considering all of these factors, we have concluded that the balance of public interest lies in upholding the exemption and not releasing the information requested. Although disclosure would provide transparency about our software systems and IT infrastructure, this is outweighed by the harm that could be caused by people who wish to use this information to assess any vulnerabilities in our security measures and consequently use this information for unlawful purposes. Cybercrime can not only lead to major service disruption but can also result in significant financial losses. As a publicly funded

organisation, we have a duty for ensuring our public funding is protected and spent responsibly. Moreover, as a public body the Trust must demonstrate that it keeps its confidential data and IT infrastructure safe and complies with relevant legislation, but at the same time we must be vigilant that transparency does not provide an opportunity for individuals to act against the Trust. In considering the impact that recent cyber-attacks have had on NHS services, including the cancellation of thousands of patient appointments and procedures as well as the loss of confidential patient data, we consider the overriding public interest lies in withholding this information. The private or commercial interests of a requester should not outweigh the public interest in protecting the integrity of our systems and continuity of our essential patient services. Although we appreciate there may be legitimate intentions behind requesting this information, we must take a cautious approach to requests of this nature and appreciate your understanding in this matter.

Section 40(2)

I can confirm that we hold this information, but it is exempt under Section 40(2) of the Freedom of Information Act 2000 – Personal Information of third parties. This is because this information may allow the identification of individuals and disclosure would breach the principles of the Data Protection Act.

This is an absolute exemption and therefore carries no requirement to consider the public interest.

Section 44

We are unable to provide the contact details of staff as we consider this information to be exempt from release in accordance with Section 44 of the Freedom of Information Act (Prohibition on Disclosure) and would refer to the Privacy and Electronic Communications EC Directive Regulations 2003 which provide specific rules on electronic communication services, including marketing (by phone, fax, email or text) and keeping communications services secure. We will not provide any information that could result in the transmission of unsolicited communications which may place an unacceptable risk to our email network and could also have a detrimental impact on patient care and treatment.

The contact number for the Trust is accessible on the Trust website <http://www.esht.nhs.uk>.

This is an absolute exemption and therefore carries no requirement to consider the public interest.

4. Please provide details of any third-party suppliers, frameworks, or managed service providers currently supporting the Trust's service desk and/or helpdesk management and clinical system support functions, including:

- **supplier name;**
- **service provided;**
- **contract start/end dates;**
- **procurement framework used (if applicable); and**
- **annual contract value where held.**

Whilst the Trust holds the information requested, it is applying a Section 43(2) exemption in relation to this part of the request, as the trust is currently in a pre-procurement process for the services mentioned.

In applying the exemption consideration has been given to the public interest in enabling scrutiny of public sector decision making and the general public interest in accountability and transparency.

We have concluded that disclosure at this stage may prejudice the pre-procurement process.

In this instance, we consider that the public interest in withholding the information is greater than the public interest in disclosing the information.

5. Please provide details of any current or planned digital transformation programmes, improvement initiatives or projects related to the delivery of IT service management, IT service desk/helpdesk and end user computing services

Replacement of the Service Desk tool.

6. Please provide details of any planned or anticipated procurement exercises, contract renewals, workforce expansion programmes, or technology investments relating to IT service management and IT service desk/helpdesk services that are currently approved or in procurement planning documentation.

We are currently in a tender process.

I trust this information is helpful in its detail or explanation however, if you are dissatisfied with the response, then you have the right to request an internal review. If you wish to seek an internal review, please write to the Freedom of Information Team at esh-tr.foi@nhs.net quoting the above FOI reference number, within 40 working days. Please note the Trust is not obliged to accept a request for an internal review after this time period.

Yours faithfully

Freedom of Information (FOI) Team
East Sussex Healthcare NHS Trust
0300 131 4716
Core Hours of Business: Monday to Friday 9.00am to 4.00pm

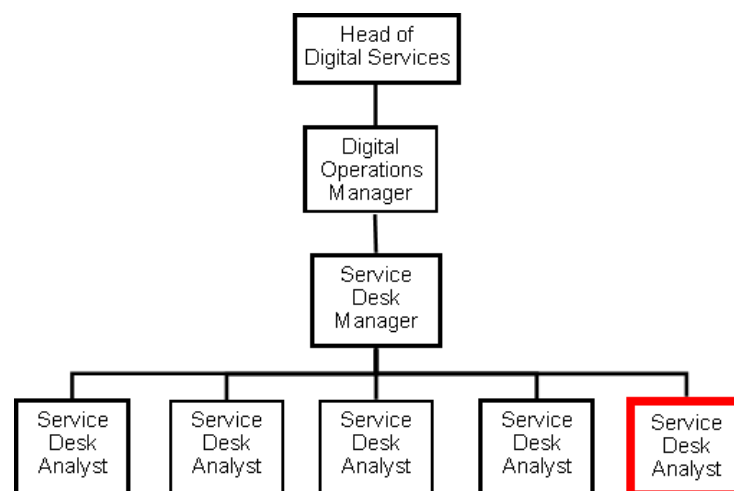
Job Description

Job Ref:	24-240
Job Title:	Service Desk Analyst
AfC Pay Band:	Band 4
Number of hours:	37.5 hours per week Please note: whilst the team currently provides a service from 8am – 6pm weekdays, the growing reliance on digital systems means that the hours of service may be extended in the future which the postholder would be expected to support within their 37.5 hours per week
Clinical Unit / Division	Finance
Department:	Digital
Location:	Eastbourne DGH
Accountable to:	Head of Digital Delivery
Reports to:	Service Desk Manager

Job dimensions & responsibility for resources	
Budgetary & Purchasing, Income generation	Budget / Delegated Budget managed: N/A Authorised signatory for: N/A Other financial responsibility: Careful use of Trust resources
Staff	Staff (wte): N/A
Information Systems	Careful use of Trust systems both manual and electronic, to ensure accuracy of data. Store and share information in accordance with department protocols, Trust Information Governance Policy and Data Protection Legislation Specialist systems: [REDACTED]

Job purpose	The postholder will be a member of the Digital Service Desk Team, providing first line technical support to all Trust staff, ensuring users can report faults, register requests and obtain information and advice. The team provides a responsive customer focussed service via incoming telephone calls and an online portal. The postholder will deal with calls and requests, providing immediate resolution to issues wherever possible and ensuring the service is delivered within agreed Service Level Agreements (SLAs). When needed, they will escalate issues and will liaise with multiple colleagues, both within Digital and across the wider Trust.
-------------	---

Department Structure



Communications and Working Relationships

With Whom:	Frequency	Purpose
Service Desk Manager	Daily / as required	Management supervision, work planning, advice and support

Service Desk Analysts	Daily / as required	Peer support and advice
Digital Operations Manager and Head of Digital Services	As required	Advice, escalation of issues
Technical teams	Daily / as required	Liaison / support to resolve issues
Trust staff (to include both clinical and non-clinical staff)	Daily	Investigation and resolution of issues, provision of support and information
Suppliers	As required	To support resolution of issues

Key duties and responsibilities

1. Respond to telephone calls from end users and record these within the Trust Incident Management System, following agreed protocols
2. Deliver a high degree of customer service for all relevant support queries and develop excellent customer relationships
3. Accurately document all support calls and emails, gathering as much information as quickly as possible to correctly diagnose faults. 'Own' the calls, following them through reporting to closure.
4. Demonstrate an effective team ethos. Demonstrate high performance standards both individually and as part of a team, in the achievement of Key Performance Indicators (KPIs) and priorities
5. Work independently to efficiently resolve customer queries, only escalating when absolutely necessary

Communication and Relationship skills

6. Demonstrate an excellent level of customer service, ensuring each caller feels supported and has the confidence that their issue will be resolved
7. Provide a responsive and customer focused service desk and first line support service to users of Digital with any issues concerning PC's, printers, etc. and associated software in non-technical language where there may be barriers to understanding
8. Demonstrate proficiency in customer service techniques and call handling, to ensure that full account is taken of end user requirements
9. Show empathy and understanding when dealing with IT shy users whilst providing guidance in line with users' abilities
10. Ensure that all support calls and requests are dealt with appropriately and in accordance with defined policies and procedures, in accordance with service level agreements.
11. Escalate urgent calls or high clinical impact calls promptly and effectively to the Digital Service Desk Manager
12. Escalate calls to second and third line support teams should a first line fix not be available or a site visit required
13. Provide support and advice to other Digital staff, Trust managers and end-users on the use and management of digital hardware and software following development and implementation

14. Provide first line fault diagnosis and fault fixing
15. Follow escalation channels, ensuring that the correct route to resolve calls is taken. If calls are passed to a third party, the postholder is required to monitor the call and ensure its correct and timely resolution
16. Keep the user informed of developments throughout the call's lifecycle; the Service Desk is the communication channel between users and Digital services

Analytical and Judgemental Skills

17. Use departmental guidelines and protocols, actively troubleshoot and/or document to identify, assess, record, resolve and/or escalate incidents and service requests ensuring they are handled in a professional and sensitive manner
18. Use knowledge of policies, procedures and IT to provide users with realistic and implementable alternatives
19. Provide feedback and input to the development of new guidelines or procedures
20. Maintain the Service Desk inventory and user/contacts database

Knowledge, Training and Experience/Planning & Organisational skills

21. Set up and configure PCs and associated equipment to the agreed specification and standard
22. Record incidents, contacts and services provided using a range of computer-based tools
23. Create and maintain IT user accounts and systems (logging username requests, creating accounts in accordance with strict governance guidelines, assigning appropriate access rights, and issuing usernames and passwords to staff)
24. Document fixes for known problems
25. Work closely with the Client Devices team to ensure a smooth end-to-end user experience and knowledge transfer between support teams
26. Assist in the maintenance of digital documentation for the department and provide supporting documentation to the business as usual support teams
27. Provide first line support for desktops, laptops, printers and other equipment for staff at the Trust. Ensure that all agreed [REDACTED] based processes and Trust and Digital policies and processes relevant for support are followed.
28. Provide advice, assurance, training and support to users in both standard desktop software and clinical systems
29. Ensure that any risks for the department are identified and escalated to the Service Desk Manager
30. Keep up to date with emerging technologies and best practice and share knowledge with professional colleagues as appropriate
31. Assist in the development of policies, standards, working practices and other quality initiatives within the team. Participate in internal working groups as necessary.
32. Carry out non-routine tasks such as development and documentation of new services, major incident process etc.

Personal/Professional Development

33. Participate in personal objective setting and review, including the creation of a personal development plan

34. Participate in ongoing training and support from second line support teams including rotational days shadowing Client Device Engineers to continue self-development and maintain a full understanding of user environments and clinical demands
35. Work alongside other Digital teams to ensure a broader knowledge transfer and ongoing working relationships across the service
36. Provide advice and demonstrate own activities to new or less experienced staff within the immediate team and the wider department
37. Implement policies for own work area and propose changes to working practices or procedures within the Service Desk environment so as to promote continuous quality improvement initiatives within the team and wider department
38. Maintain own mandatory training record in line with the Trust's guidelines
39. Achieve and demonstrate agreed standards of personal and professional development within agreed timescales

Health & Safety

40. Ensure that duties are carried out in accordance with health and safety regulations. The postholder should not endanger the health and safety of him/herself or others whilst at work.
41. Take reasonable care for your own Health and Safety and that of any other person who may be affected by your acts or omissions at work

Confidentiality

42. Ensure that confidentiality is maintained and Trust Information Governance policies are followed at all times
43. Be aware of Caldicott and principles around information governance

Equality and Diversity

44. Promote equality and diversity in your working life, ensuring that all staff who you work with feel valued and are treated in a fair and equitable manner

General Duties & Responsibilities applicable to all job descriptions

- To be familiar with and adhere to the policies and procedures of the Trust.
- Behave and act at all times in accordance with the Trust Values of Kindness, Integrity and Inclusivity
- To achieve and demonstrate agreed standards of personal and professional development within agreed timescales.
- To participate fully in the performance and development review (appraisal) process and undertake Continuing Professional Development as required.
- To participate in surveys and audits as necessary in order to enable the Trust to meet its statutory requirements.
- To be aware of the Trust's emergency planning processes and follow such processes as necessary, in the event of an unexpected incident.
- This job description is not exhaustive. Staff may be required to undertake any other duties at the request of the line manager, which are commensurate with the band, including project work, internal job rotation and absence cover.

Working Environment:					
Driving		Lifting		Verbal aggression	X
Use of PC/VDU	X	Physical support of patients		Physical aggression	
Bending/kneeling		Outdoor working		Breaking unwelcome news to others	
Pushing/pulling		Lone working		Providing professional emotional support	
Climbing/heights		Chemicals/fumes		Dealing with traumatic situations	
Repetitive movement	X	Contact with bodily fluids		Involvement with abuse cases	
Prolonged walking/running		Infectious materials		Care of the terminally ill	
Controlled restraint		Noise/smells		Care of mentally ill & challenging patients	
Manual labour		Waste/dirt		Long periods of concentration i.e. hours	X
Food handling		Night working		Working in confined spaces (eg roof spaces)	

Statement

1. This job description will be agreed between the jobholder and the manager to whom he/she is accountable. It may be reviewed in light of experience, changes and developments.
2. The information being handled by employees of East Sussex Healthcare NHS Trust is strictly confidential. Failure to respect the confidential nature of this information will be regarded as a serious breach of regulations, which will result in action under the Disciplinary Procedure, including possible dismissal. This includes holding discussions with colleagues concerning patients in situations where the conversation may be overheard. It is the employee's personal responsibility to comply with the Data Protection Act.
3. It is the employee's responsibility to ensure all records (computerised or manual) are accurate and up to date, and that errors are corrected or notified as appropriate.
4. It is the manager's role to monitor and assure the quality of any data collected or recorded by or in his/her area of responsibility.
5. Employees must take reasonable care, and be aware of the responsibilities placed on them under the Health & Safety at Work etc. Act (1974) and to ensure that agreed safety procedures are carried out to maintain a safe environment for employees, patients and visitors.
6. All staff have a responsibility to ensure that infection control policies, procedures and guidelines are adhered to, in addition to supporting the trusts commitment to preventing and controlling healthcare associated infections (HAI).
7. All members of staff must be aware of their responsibilities under the Freedom of Information Act 2000.
8. In addition to any specific responsibility for risk management outlined in the main body of this job description, all employees must ensure they are aware of the key responsibilities

applicable in relation to risk management as identified in the Trust's Risk Management Strategy.

9. All staff will note the Trust's responsibilities under the Civil Contingencies Act 2004, and NHS Major Incident Plans Guidance (DoH 1998 and 2004)
10. All employees are responsible for ensuring they attend the relevant mandatory training as identified in the Trust's Education Strategy and as agreed with their manager/supervisor.
11. It is the employee's responsibility to ensure they follow the latest version of all policies and procedures which apply to them.
12. For posts which involve contact with patients, it is required that the postholder receives satisfactory clearance from the Disclosure and Barring Service.

Job Title: Service Desk Analyst	Grade: Band 4		
Department: ESHT Digital	Date: September 2024		
*Assessed by: A= Application I= Interview R= References T= Testing C = Certificate			
Minimum Criteria	*	Desirable Criteria	*
Qualifications			
- Educated to NVQ Level 4 / Diploma level or equivalent in Computing or IT related subject to include administration and customer service skills - Proven level of literacy and numeracy – GCSE grade C or above	A/I A/I	Understanding of [REDACTED] framework and processes	A/I
Experience			
- Customer Service telephone call handling experience - Experience of delivery to key targets - Experience of working with suppliers from a range of technical functions such as servers, desktops, network etc. - Experience of working in team environments	A/I A/I A/I A/I	- Experience of working within the NHS - Awareness of NHS Information Governance principles	A/I A/I
Skills / Knowledge / Abilities			
- Knowledge of [REDACTED] service support processes and practices including the application of quality and performance standards - Intermediate knowledge of computer hardware and software - A technical appreciation and understanding to diagnose a	A/I A/I A/I	- Understanding of the NHS Constitution - Understanding of NHS environments and the IT systems involved, e.g. [REDACTED]	A/I A/I

broad range of desktop equipment faults • Knowledge of desktop and mobile data technology and proficiency in the use of office automation or productivity packages such as [REDACTED] and email • General understanding of IT / IG guidance/regulations that apply to the NHS, including Freedom of Information Act 2000, Data Protection Act 1998, Caldicott Guidelines and Data Accreditation Standard. • Ability to work within strict procedures and protocols, ensuring IT security procedures are followed • Good keyboard and Microsoft Office skills • Excellent communication skills with a wide range of users including the ability to communicate technical information • Ability to interpret Trust policies and procedures and be able to communicate this interpretation to end users • Ability to be able to assess the needs of a situation from the facts presented by the end user and analyse a range of solutions to ensure a successful conclusion of the call • Good customer service skills, including the ability to maintain a professional approach under all circumstances, particularly with people who are stressed or angry • Self-motivated with ability to work unsupervised, plan own workload and independently adjust to call volume requirements • A logical, analytical approach to problem solving paying close attention to detail	A/I A/I A/I A/I A/I A/I A/I A/I	• Ability to delegate duties to other team members when appropriate • Able to move IT equipment such as desktop computers, printers etc.	
--	---	---	--

• Able to keep accurate work records • Diligent and diagnostic approach to problem solving • A flexible, responsible attitude and approach to work with the ability to work after normal working hours when required • Flexible in their attitudes and behaviours to support team working and delivery of objectives	A/I A/I A/I A/I		
Other • Reliable work record • <i>DBS clearance if applicable</i> • Evidence that personal behaviour reflects Trust Values	AI T AIR		

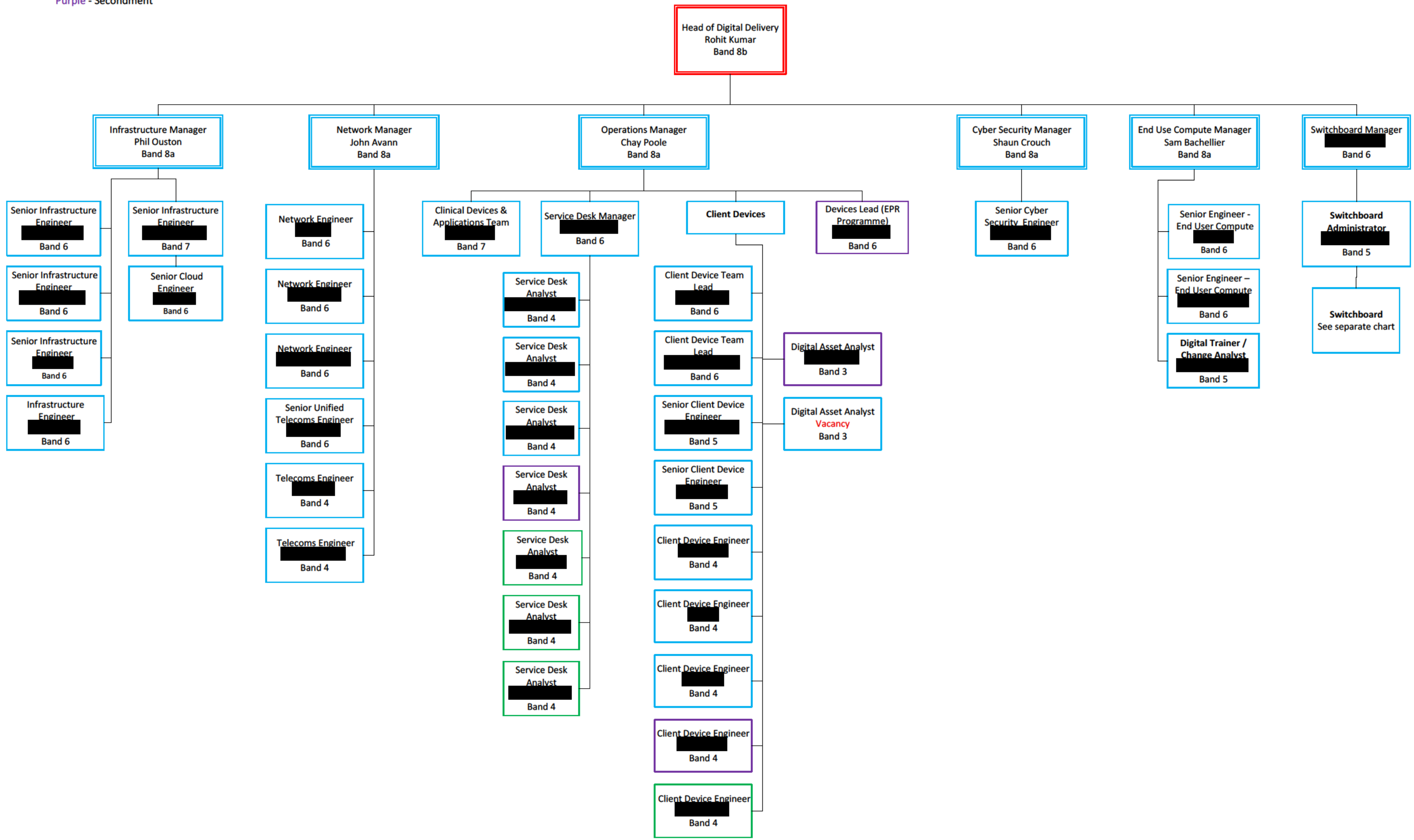
Managers Signature

Date

Postholder's signature

Date

Key
Red – Senior Team Member
Blue – Substantive Post
Green – Fixed Term
Purple - Secondment



Job Description

Job Ref:

Job Title: IT Operations Manager

AfC Pay Band: Band 8a

Number of hours: Full time 37.5 hours per week

Division: Finance

Department: Digital

Location: Based at Conquest or Eastbourne DGH site, working across all sites as required

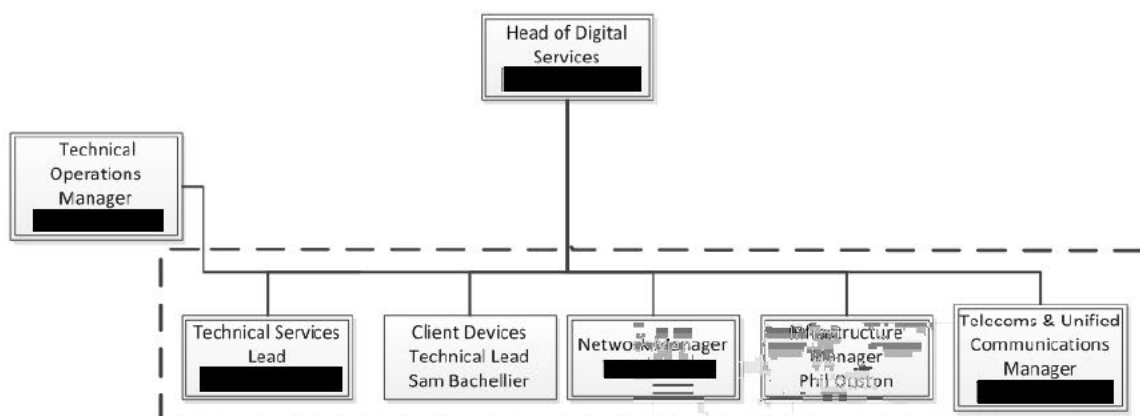
Accountable to: Associate Director of Digital

Reports to: Head of Digital Services

Job dimensions & responsibility for resources	
Budgetary & Purchasing, Income generation	Signatory for authorising expenses and time sheets.
Staff	Technical Leads, Senior Infrastructure Engineers, and Telecoms Engineers
Information Systems	

Job purpose	Reporting to the Head of Digital Services ensuring clear leadership and delivery of operational support services. The post holder will be key to the overall success of Digital operational services. They will be responsible for IT service availability while ensuring that the operational performance of support services meets agreed KPIs. In addition the post holder will ensure projects and other work requests assigned to Infrastructure, networking and Client devices services are appropriately resourced and delivered in line with Trust priorities. This role leads by example and acts as a force driving high standards throughout the department not limited by the immediate line management responsibilities of the post. Providing strong leadership and hands on management on a daily basis to ensure the delivery of a high standard of IT services to the users of the service. In particular the post holder will develop a strong performance culture promoting the values that reflect the high standards required to deliver effective IT services. Contributing to the development of strategic technology plans and policies the post holder will have specific responsibility to provide leadership on service improvement and innovation. In particular this role will lead on ITIL service management improvements. Out of hours support is provided by the department and active participation in this is a requirement of the post.
-------------	--

Department Structure:



KEY DUTIES AND RESPONSIBILITIES:

Operational

1. Act as the lead for operational services supporting the review, development and implementation of a range of service, policies and standards applicable to information technology support services
2. Overseeing technical staff ensuring standards and procedures are in place and adhered to
3. Act as the senior lead for the department on programmes and projects
4. To provide advice supporting business planning and the development of strategic technical roadmaps
5. Ensure security compliance standards are met in accordance with Trust policies
6. To identify key risks and escalate them in accordance with Trust procedures as appropriate
7. Develop and improve service management practices
8. Provide and maintain evidence to support information security reviews and best practice including Trusts Information Security Management System
9. Approve expenditure for maintenance and repair of equipment
10. Ensuring license compliance is adhered to
11. Contribute to and develop disaster recovery plans

Personnel Functions

1. Carry out appraisals for senior technical staff
2. Lead on planning training requirements across the department to ensure staff professional development meet trust strategic plans
3. Approve staff payments including on call, overtime and expense payments.
4. Co-ordinate and report annual leave and communicate sick leave on a monthly basis.
5. Co-ordinate, book and record attendance of annual statutory training for the team.

Leadership

1. Provide leadership and management to operational teams to achieve high performance and effective operational delivery
2. Provide guidance and assistance in the equitable distribution of work to team members and the re-allocation of this workload in the event of absence.
3. Ensure an efficient and proactive customer service.
4. Uphold professional standards and act as advocate for the Department.
5. Maintain a highly organised office environment to maintain confidentiality and data protection and set office standards for the team.
6. Maintain and develop an environment and culture that improves health, safety and security of the work place, ensuring effective risk management strategies are implemented.

Communication

1. Liaise appropriately with external product suppliers and contractors to influence the outcome of decisions ensuring that the Trusts needs are met and that technological solutions are appropriately matched to current and planned infrastructure plans and IT strategies.
2. Work closely with all areas of the department to ensure cohesive strategies in the delivery of products and services, including the appropriate standardisation of technology products
3. Present complex technical information clearly to colleagues at all levels.
4. Ensure that confidentiality is maintained at all times and that staff adhere to the Data Protection Act, Freedom of Information Act and the Caldicott Principles.

Policy and Service Development

1. Develop policies and procedures for effective implementation and maintenance of IT services supporting operational service levels and department strategic aims
2. Work with the Head of Digital Services to ensure that there is full compliance with department policies and procedures, such that the targeted service levels are achieved and strategic aims met
3. Identify areas for improvement in systems, processes and procedures that will improve the service, seeking agreement and taking issues forward with appropriate support.
4. Working with the relevant stakeholders both internal and external to the Trust, lead on the implementation of compliant IT services

Administrative

1. Ensure that all system management and security tasks and procedures are fully documented (and accessible by others) and that cross cover procedures are maintained so that all tasks can be completed in the absence of the post holder, whether planned or unplanned.
2. Carry out staff appraisals and support on going professional development
3. Assist in the formulation of annual operational plans and budgets for capital planning ensuring there are clear priorities.
4. Contribute to department and Trust business cases as necessary with proposed technical approaches

Training and Education

1. To attend ESHT NHS Trust mandatory training and that accurate records are maintained of all training attended by individual staff members.
2. To act as a mentor for new team members, supervising their training and monitoring the induction programme.
3. Co-ordinate training workshops for the team, covering new developments within the service.

Audit and Research

1. To oversee and carry out audit activity, to ensure good practice within the department.
2. Undertake and manage project work under own initiative, including analysis and interpretation of data and results and assessment of options.

Personal and Professional Development

1. Commitment to improve skill levels and knowledge by participation in appropriate training and learning opportunities.
2. Attend mandatory and statutory training as required.

3. Attend relevant education, training and study days as required.
4. Responsible for maintaining own professional development including being aware of new developments within the sphere of the role.
5. Be mindful of, and do whatever possible, as appropriate to this role and level of responsibility, to enable ESHT to fulfil their statutory duty to ensure that patients, clients and members of the public are consulted and involved in decisions about local health service developments.

Other Role-Specific Duties

1. To be familiar with and adhere to the policies and procedures of the Trust.
2. Behave and act at all times in accordance with the Trust Values, of Working Together, Respect and Compassion, Engagement and Involvement and Improvement and Development
3. To achieve and demonstrate agreed standards of personal and professional development within agreed timescales.
4. To participate fully in the performance and development review (appraisal) process and undertake Continuing Professional Development as required.
5. To participate in surveys and audits as necessary in order to enable the Trust to meet its statutory requirements.
6. To be aware of the Trust's emergency planning processes and follow such processes as necessary, in the event of an unexpected incident.
7. This job description is not exhaustive. Staff may be required to undertake any other duties at the request of the line manager, which are commensurate with the band, including project work, internal job rotation and absence cover.

Working Environment:

Driving	√	Lifting		Verbal aggression	
Use of PC/VDU	√	Physical support of patients		Physical aggression	
Bending/kneeling		Outdoor working		Breaking unwelcome news to others	
Pushing/pulling		Lone working	√	Providing professional emotional support	√
Climbing/heights		Chemicals/fumes		Dealing with traumatic situations	
Repetitive movement		Contact with bodily fluids		Involvement with abuse cases	
Prolonged walking/running		Infectious materials		Care of the terminally ill	
Controlled restraint		Noise/smells		Care of mentally ill & challenging patients	
Manual labour		Waste/dirt		Long periods of concentration i.e. hours	√
Food handling		Night working		Working in confined spaces (eg roof spaces)	

Statement

This job description will be agreed between the jobholder and the manager to whom he/she is accountable. It may be reviewed in light of experience, changes and developments.

The information being handled by employees of East Sussex Healthcare NHS Trust is strictly confidential. Failure to respect the confidential nature of this information will be regarded as a serious breach of regulations, which will result in action under the Disciplinary Procedure, including possible dismissal. This includes holding discussions with colleagues concerning patients in situations where the conversation may be overheard. It is the employee's personal responsibility to comply with the Data Protection Act.

It is the employee's responsibility to ensure all records (computerised or manual) are accurate and up to date, and that errors are corrected or notified as appropriate.

It is the manager's role to monitor and assure the quality of any data collected or recorded by or in his/her area of responsibility.

Employees must take reasonable care, and be aware of the responsibilities placed on them under the Health & Safety at Work etc. Act (1974) and to ensure that agreed safety procedures are carried out to maintain a safe environment for employees, patients and visitors.

All members of staff must be aware of their responsibilities under the Freedom of Information Act 2000.

In addition to any specific responsibility for risk management outlined in the main body of this job description, all employees must ensure they are aware of the key responsibilities applicable in relation to risk management as identified in the Trust's Risk Management Strategy.

All staff will note the Trust's responsibilities under the Civil Contingencies Act 2004, and NHS Major Incident Plans Guidance (DoH 1998 and 2004)

All employees are responsible for ensuring they attend the relevant mandatory training as identified in the Trust's Education Strategy and as agreed with their manager/supervisor.

It is the employee's responsibility to ensure they follow the latest version of all policies and procedures which apply to them.

For posts which involve contact with patients, it is required that the postholder receives satisfactory clearance from the Disclosure and Barring Service.

Person Specification

Job Title: Digital Operations Manager	Grade: 8a
Department: ESHT Digital	Date: July 2018

*Assessed by: A= Application I= Interview R= References T= Testing C = Certificate

Qualifications	In-depth knowledge of IM&T systems and procedures acquired through a combination of specialist training and relevant study to master's degree or equivalent level, (E)
Professional Registration	
Knowledge and Experience	
Non-clinical	Proven Experience in managing successful IT services (E) Experience in implementing strategic IM&T plans and technical road maps (E) Experience of managing technical staff. (E) Knowledge of enterprise level networking solutions (E) Knowledge of Enterprise level wireless network technology (E) Knowledge of Enterprise Level network access control principles and technology (E) Knowledge of Enterprise level network security (E) Knowledge of Microsoft Active Directory services (E) Knowledge of Virtual hosting platforms (E) Knowledge of Enterprise level SAN storage technology (E) Knowledge of Enterprise Level back up technology (E) Knowledge of Data base technologies (E) Knowledge of software deployment and release management (D) Knowledge of Microsoft Operating Systems (E) Knowledge of Desk top security software (E) Knowledge of Data Protection/Caldicott, (D) Experience of information security (E) Experience of information governance (D). Knowledge of current NHS strategies and policies. (D) Experience of implementing complex projects (D) Experience of ITIL framework(E) Knowledge of ISO standards (D)

Clinical (where appropriate)	
Skills and Abilities	
Communication and Interpersonal	Excellent written and spoken English and interpersonal/negotiating skills. Able to establish and maintain working relationships with colleagues from a variety of professional and organisational backgrounds. Able to present extremely complex and highly technical information clearly to colleagues at all levels and to present cases that inform decision making and to influence this decision making to ensure that the correct decisions are made. Able to persuade and influence people in appropriate courses of action for solutions to extremely complex problems that potentially cross boundaries within the organisation. Proven ability to influence others to support the success maintenance and commissioning of technical services. Able to write a range of I.T. policies and strategy documents in a clear concise manner. Effective interpersonal skills.
Analytical and Judgemental	Expert knowledge of interpreting requirements and designing and developing complex solutions. To monitor and interpret extremely complex IT issues that may have no precedent and take appropriate action to resolve and negate risk Able to field and resolve complex issues and queries from other team members and to effectively deal with these. Proactive approach to problem-solving and proven ability to develop and implement solutions to complex problems.
Planning and Organisational	Excellent time management and ability to deliver accurate work within strict timescales. Also able to plan, organise and prioritise the time of other team members when necessary. Able to manage conflicting priorities of self and others on a daily basis. Able to define own and other team members objectives without reference to management and act on them. Able to work to tight deadlines and prioritise and re-prioritise workloads of self and others as necessary, depending on service demands and resources. Ability to manage a number of diverse and complex programmes of work simultaneously.
Financial	Authorised signatory; responsible for the purchase of some physical assets and supplies; installation and/or repair and maintenance of physical assets Signs off overtime expenses; authorises purchase of IM&T equipment; responsible for the installation or repair and maintenance of IM&T equipment
Information and Communication Technology	Use of Microsoft Office
Supervisory and HR Management	Day to day coordination/Management of staff; teach/deliver specialist training Leads and contributes to staff appraisal and professional development for technical staff
Freedom to Act	Works autonomously with reference to policies and guidelines but may need to interpret these and advise on how they should be applied and implemented. Provides advice on complex subjects and issues without referring to a manager. Acts as a subject matter expert within Digital Development.
Physical	No significant physical effort required. The role is mainly desk based

Mental	Concentration required when analysing IM&T issues, interruptions to answer queries from staff, customers Ability to manage multiple IM&T requests running simultaneously and to switch attention between tasks as required. Ability to spend a number of hours concentrating on a task including spending long periods working on a VDU.
Emotional	Able to handle periods of high pressure with the ability to lead and take the initiative
Working Conditions	Office conditions VDU
Personal Attributes	Highly motivated and able to motivate others. Able to maintain composure during times of extreme pressure. Commitment to providing a quality service and continuous improvement. Attention to detail and the ability to see tasks through to their completion

Managers Signature

Date

Postholder's signature

Date

Job Description

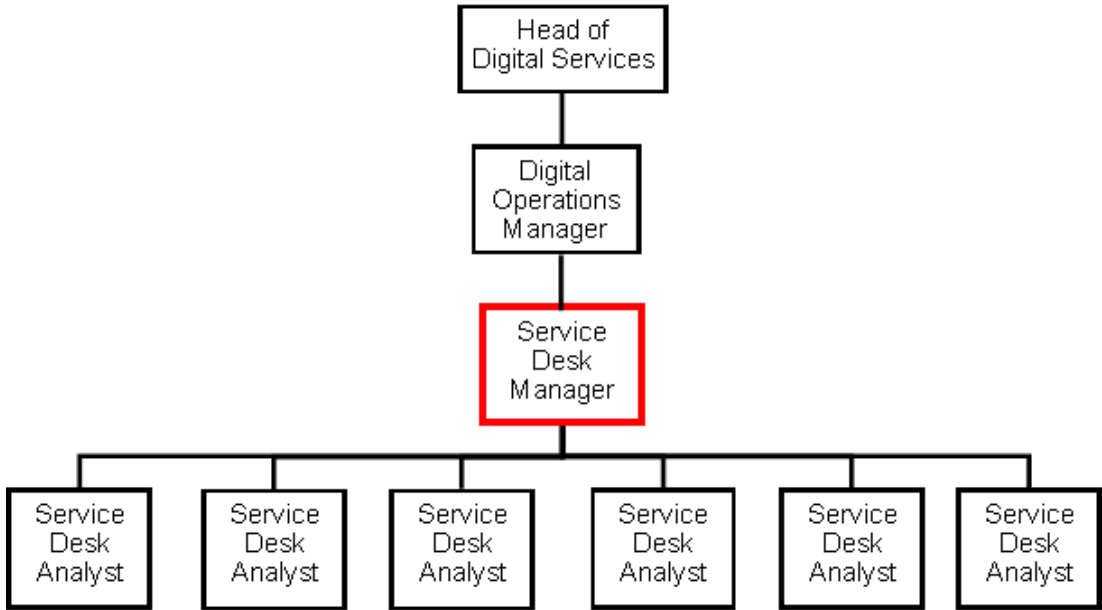
Job Ref:	22-317
Job Title:	Service Desk Manager
AfC Pay Band:	Band 6
Number of hours:	37.5
Clinical Unit / Division	Finance
Department:	Digital
Location:	Eastbourne DGH
Accountable to:	Head of Digital Services
Reports to:	Digital Operations Manager

Job dimensions & responsibility for resources	
Budgetary & Purchasing, Income generation	Authorisation of overtime and Bank timesheets Careful use of Trust resources.
Staff	Direct management of up to 6 WTE staff members (Service Desk Analysts) plus Bank staff as required
Information Systems	Careful use of Trust systems both manual and electronic, to ensure accuracy of data. Store and share information in accordance with department protocols, Trust Information Governance Policy and Data Protection Legislation Specialist systems: Call Centre Supervisor, [REDACTED] Service Desk including Reporting elements, [REDACTED] [REDACTED]

Job purpose	The Service Desk Manager is responsible for the day-to-day management of the ESHT Digital Service Desk in accordance with the agreed policies and procedures. This requires the supervision and development of the Service Desk team to ensure that users are able to report faults, register requests and obtain advice and information and receive a high quality service
-------------	--

	provided in accordance with SLA (Service Level Agreement), Key Performance Indicators and OLA (Operational Level Agreement) The postholder will be responsible for scheduling the team's resources and developing staff to agreed levels of competency. They will provide statistical information, monitoring and reporting on performance of the Service Desk which will feed into the monthly Digital Integrated Performance Review and other reporting as required. The postholder will act as an escalation point for complex technical issues and will investigate and respond to any complaints received by the department. They will also be expected to continuously look for ways to develop and improve the service provided by the team and ensure that the team fulfils its role as set out in the Digital Major Incident Plan in the event of a serious incident.
--	--

Department Structure



Communications and Working Relationships		
With Whom:	Frequency	Purpose
Service Desk Analysts	Constantly	Supervise, work planning, advise, supporting.
Client Devices Team	Daily / Hourly / as required	2 nd Line Support work planning advice.
Infrastructure Team	Daily / Weekly / as required	2 nd Line Support work planning advice.
Network Team	Daily / Weekly / as required	2 nd Line Support work planning advice.
Digital Operations Manager	Daily / Hourly / as required	Line Manager, work planning, advice, support.
Head of Digital Operations	As Required	Advice & Support
Associate Director of Digital	As Required	Advice & Support
Digital Senior Leadership Team	As Required	Contribution to the overall development of Digital
Information Security Team	As Required	Advice

Key duties and responsibilities

Communication

1. Communicate effectively with all users of the service in a positive and helpful manner, providing specialist advice along with timely updates and service notifications
2. Able to present and explain complex information to non-technical colleagues in a clear and concise way, ensuring that understanding is gained
3. Escalate calls to 2nd and 3rd level support functions, communicating very detailed and technical information to colleagues within ESHT Digital
4. Liaise with counterparts in other NHS Trusts as necessary to ensure the resolution of support calls that go beyond the Trust
5. Act as a role model for junior staff in the team by demonstrating excellent communication and listening skills
6. Work with stakeholders to plan for service disruption and/or breaches of service level agreements

People Management

7. Line management of Service Desk team members
8. Delegate work to team members as appropriate, planning, organising and prioritising their time where necessary
9. Ensure that all team members have regular 1:1 meetings and an annual appraisal where objectives are set, development/training needs are identified and career progression is discussed

10. Authorise annual leave, ensuring appropriate resourcing so that operational effectiveness is maintained
11. Manage sickness and other absence in line with Trust policy
12. Manage disciplinary matters for members of the team
13. Ensure that the team have been adequately trained and have the appropriate skills to complete the tasks required
14. Coach team members, using feedback from the user satisfaction survey, to improve performance
15. Responsible for recruitment of team members and for training new members of staff when they join the team
16. Ensure that all team members have completed their mandatory training, scheduling time for them to complete this if necessary

Service Delivery and Improvement

17. Ensure all calls, which will include specialist and complex digital information, are processed in accordance with the agreed policies and procedures and that users receive a high quality service, which is provided in accordance with Service Level Agreements and Key Performance Indicators
18. Act as the escalation point for complex technical issues, investigating these and comparing possible options and configuring software/hardware before proposing solution/providing resolution
19. Make informed decision on further escalation of issues to 2nd and 3rd line support, explaining the complex detail to colleagues
20. Analyse data to provide statistical information on the performance of the team and use this data to propose changes and identify areas for improvement
21. Investigate and respond to any complaints received about the team and service provided
22. Responsible for creating and writing Service Desk Policies, Procedures and Standard Operating Procedures and the approval and ratification of these
23. Continuously look for ways to develop and improve the service provided by the team, including the ongoing development of the online portal, ensuring that the service is developed in line with the Trust's Digital Strategy
24. Carry out regular research and evaluation of new working practices and supporting toolsets for use in the Trust
25. Attend the weekly Change Advisory Board (CAB), identifying where proposed changes may impact on the Service Desk and cascade to the team any change that may impact on users
26. During any major incident, ensure the team fulfils its role as set out in the Digital Major Incident Plan, ensuring effective communications are in place and that the team supports Digital colleagues as they work towards a resolution
27. Participate in Major Incident reviews as necessary
28. Provide reports as required to Digital Operations Manager and Head of Digital Services
29. Work with Information and Cyber Security team to promote best practice with Trust users.
30. Identify gaps in the available information required to understand a problem or situation and devising a means of resolving them
31. Assist with the specification, development, research and evaluation of customer services standards.
32. Participate in analysis of customer satisfaction surveys and data and identifies actions for service improvements where appropriate. Supports and participates in regular review meetings between service providers and customers/users.
33. Analyse, investigate and resolve complex Digital queries this also could involve multiple incidents which may have an underlying problem which will need to be identified Acquire a proper understanding of a problem or situation by breaking it

down systematically into its component parts and identifying the relationships between these parts.

General Duties & Responsibilities applicable to all job descriptions

- To be familiar with and adhere to the policies and procedures of the Trust.
- Out of hours support is provided by the department and active participation in this is a requirement of the post
- Behave and act at all times in accordance with the Trust Values, of Working Together, Respect and Compassion, Engagement and Involvement and Improvement and Development
- To achieve and demonstrate agreed standards of personal and professional development within agreed timescales.
- To participate fully in the performance and development review (appraisal) process and undertake Continuing Professional Development as required.
- To participate in surveys and audits as necessary in order to enable the Trust to meet its statutory requirements.
- To be aware of the Trust's emergency planning processes and follow such processes as necessary, in the event of an unexpected incident.
- This job description is not exhaustive. Staff may be required to undertake any other duties at the request of the line manager.

Working Environment:

Driving		Lifting		Verbal aggression	✓
Use of PC/VDU	✓	Physical support of patients		Physical aggression	
Bending/kneeling		Outdoor working		Breaking unwelcome news to others	
Pushing/pulling		Lone working		Providing professional emotional support	✓
Climbing/heights		Chemicals/fumes		Dealing with traumatic situations	✓
Repetitive movement		Contact with bodily fluids		Involvement with abuse cases	
Prolonged walking/running		Infectious materials		Care of the terminally ill	
Controlled restraint	✓	Noise/smells		Care of mentally ill & challenging patients	
Manual labour		Waste/dirt		Long periods of concentration i.e. hours	✓
Food handling		Night working		Working in confined spaces (eg roof spaces)	

Statement

1. This job description will be agreed between the jobholder and the manager to whom he/she is accountable. It may be reviewed in light of experience, changes and developments.
 2. The information being handled by employees of East Sussex Healthcare NHS Trust is strictly confidential. Failure to respect the confidential nature of this information will be regarded as a serious breach of regulations, which will result in action under the Disciplinary Procedure, including possible dismissal. This includes holding discussions with colleagues concerning patients in situations where the conversation may be overheard. It is the employee's personal responsibility to comply with the Data Protection Act.
 3. It is the employee's responsibility to ensure all records (computerised or manual) are accurate and up to date, and that errors are corrected or notified as appropriate.
 4. It is the manager's role to monitor and assure the quality of any data collected or recorded by or in his/her area of responsibility.
 5. Employees must take reasonable care, and be aware of the responsibilities placed on them under the Health & Safety at Work etc. Act (1974) and to ensure that agreed safety procedures are carried out to maintain a safe environment for employees, patients and visitors.
 6. All staff have a responsibility to ensure that infection control policies, procedures and guidelines are adhered to. In addition to supporting the trusts commitment to preventing and controlling healthcare associated infections (HAI).
 7. All members of staff must be aware of their responsibilities under the Freedom of Information Act 2000.
 8. In addition to any specific responsibility for risk management outlined in the main body of this job description, all employees must ensure they are aware of the key responsibilities applicable in relation to risk management as identified in the Trust's Risk Management Strategy.
 9. All staff will note the Trust's responsibilities under the Civil Contingencies Act 2004, and NHS Major Incident Plans Guidance (DoH 1998 and 2004)
 10. All employees are responsible for ensuring they attend the relevant mandatory training as identified in the Trust's Education Strategy and as agreed with their manager/supervisor.
 11. It is the employee's responsibility to ensure they follow the latest version of all policies and procedures which apply to them.
 12. For posts which involve contact with patients, it is required that the post holder receives satisfactory clearance from the Disclosure and Barring Service.
-

Person Specification

Job Title: Service Desk Manager		Grade: 6	
Department: ESHT Digital		Date: January 2024	
*Assessed by: A= Application I= Interview R= References T= Testing C = Certificate			
Minimum Criteria	*	Desirable Criteria	*
Qualifications - Degree in relevant Digital discipline or equivalent level of relevant experience - Proven experience delivering high quality, responsive services as a Service Desk Manager - Service Management certified - Evidence of continued professional development	A/C	- Project Management - Microsoft accreditation	A/I
Experience - Experience of the management of a customer facing service desk or call centre environment - Experience of delivering a service to agreed levels of performance - Experience of managing and developing a team - Experience of investigating complex technical issues and comparing options before providing resolution - Experience of leading cycle of improvement within team - Experience of writing policies and procedures	A/I	Experience of working within and IT environment with the NHS or other public sector organisation	A/I
Skills, Knowledge & Abilities - Excellent written and verbal communication skills - Able to work with people at all levels of the organisation - Able to explain complex IT information in a way that both technical and non-technical colleagues will understand - Strong knowledge of & principles	A/I	- Experience with managing major incidents - Experience of attending and participating in a Change Board	A/I

• Knowledge and experience ISO9001 & Service Desk Institute • Able to analyse data for reporting and use this to inform service improvements • Able to write reports for senior management • Knowledge of Microsoft operating systems • Excellent keyboard skills • Able to remain calm during times of pressure			
Freedom to Act • Able to manage own workload amidst changing priorities/ competing demands • Able to make informed decision on when work should be escalated to other teams • Able to delegate work to own members of staff • Delivery of objectives for self and team	A/I		
Other • Reliable work record • DBS clearance • Evidence that personal behaviour reflects Trust values			

Managers Signature

Date

Postholder's signature

Date