JOB DESCRIPTION

TITLE: **Group Infrastructure and Security Engineer**

GRADE: **Scale 10**

RESPONSIBLE TO: **Group Director: IT Services**

RESPONSIBLE FOR: N/A

PURPOSE OF THE JOB:

To administrate, manage and support multi-site network systems to ensure a single cohesive network model is consistent across all the College's campuses to include but not limited to: wide area networks, network and security platforms, storage, backups and DR/BCP.

To provide support for all College systems to IT Services team members.

MAIN TASKS AND RESPONSIBILITIES:

1. In common with all other staff:

1.1 To support the College's mission, vision, values and strategic objectives.

1.2 To implement the College's Equality and Diversity policies and to work actively to overcome discrimination on grounds of all protected characteristics; sex, race, religion/belief, disability, sexual orientation, age, pregnancy/maternity, gender reassignment status, marriage/civil partnership status.

1.3 To take responsibility for one's own professional development and participate in relevant internal and external activities.

1.4 To implement the College's safeguarding policies and practices.

1.5 To implement your health and safety responsibility in line with the College's Health and Safety policy.

1.6 To contribute to the College's commitment to continuous improvement as identified in the College's quality assurance systems.

1.7 To ensure that data is handled in line with the General Data Protection Regulations.

2. In common with all other support staff:

2.1 To participate in College-wide projects and tasks.

2.2 To work in other support services areas to meet the specific needs of workload peaks.

2.3 Such other duties of a similar nature commensurate with the grade as may be required from time to time. This may/will require working in other campuses of the College.

3. Particular to the post:

3.1 Take technical ownership of the College's multi-site virtual infrastructure and VDI platforms (VMware vSphere and Omnissa Horizon)

3.2 Act as the senior technical escalation point for complex infrastructure issues, providing hands-on diagnosis and resolution where required.

3.3 Design, operate, and improve the College's LAN and WAN services across multiple campuses, ensuring resilience, performance, and security within agreed standards (Juniper based environment)

3.4 Lead investigation and root cause analysis for high-impact or recurring network issues, driving permanent fixes rather than short-term workarounds.

3.5 Own the operational delivery of Microsoft 365 and Entra services, including identity, access control, security configuration and service reliability

3.6 Maintain and improve hybrid identity services integrating on-premise

Active Directory with cloud platforms, ensuring consistency and security.

3.7 Take operational ownership of infrastructure and cloud security controls, maintaining awareness of emerging threats and leading remediation activity.

3.8 Identify infrastructure and security risks and develop clear, evidence-based improvement proposals, including technical options, impact and risk mitigation, for formal review and approval.

3.9 Act as a senior technical point of reference for the wider IT Services team, supporting engineers through mentoring, escalation support, and knowledge sharing.

3.10 Work closely with architects, managers, and third party suppliers to ensure solutions align with agreed standards, security requirements and strategic direction.

3.11 Responsible for ensuring that all work is undertaken strictly in accordance with college safety and security procedures.

3.12 To perform manual lifting, where required, in the course of the role.

3.13 Any other duties appropriate to IT as required by the Group Director IT Services.

4. Person Specification

Essential technical skills and experience:

- Strong experience operating enterprise infrastructure within a complex, multi-site environment, including virtualised platforms, networking, identity, and core services.
- **Demonstrable hands-on experience in at least two (but not necessarily all) of the following technical areas:**

  Virtualisation and VDI platforms (VMware vSphere, Omnissa Horizon)

  Enterprise network infrastructure (LAN/WAN), ideally within Juniper-based environments

  Identity and access management platforms (Active Directory, Entra ID, Microsoft 365)

  Infrastructure and cloud security controls
- Proven ability to diagnose complex technical issues, perform root cause analysis, and lead effective resolution.
- Experience producing technical documentation, including designs, implementation plans, risk assessments and operational runbooks.
- Strong understanding of modern Windows Server environments, Active Directory, and core networking protocols (TCP/IP, DNS, DHCP)

- Strong understanding of network security principles, including firewall policy design, traffic inspection, and secure inter-network connectivity in enterprise environments.
- Experience working within formal change, incident, and problem management processes.

Security and risk

- Practical experience operating and supporting security controls across infrastructure and cloud platforms.
- Ability to identify technical risks and translate them into clear improvement proposals suitable for review through governance and change processes.
- Experience applying security controls at the network layer, including firewalls and segmentation, to manage risk and protect services.
- Experience contributing to security incidents, remediation activity, and post-incident reviews.

Automation and optimisation

- Experience using scripting or automation (e.g. PowerShell) to improve operational efficiency, reliability, or consistency.
- A pragmatic and systematic approach to platform optimisation, balancing stability, security, and operational overhead.

Desirable skills and experience

- Experience with Juniper networking technologies in large or multi-campus environments.
- Experience supporting VDI environments at scale.
- Exposure to enterprise backup, disaster recovery, and business continuity solutions.
- Experience working with endpoint management platforms (e.g. SCCM, Intune, Jamf)
- Familiarity with security assessment or auditing tools (e.g. PingCastle, Nessus)
- Experience configuring and supporting enterprise firewall platforms and network security controls (vendor-agnostic)
- ITIL or equivalent service management experience

Personal attributes

- Able to operate effectively as a senior technical contributor, providing guidance and advice without formal line management authority
- Comfortable working across multiple stakeholders, including technical and non-technical colleagues.
- Highly organized, able to manage competing priorities, and remain effective under pressure
- Proactive, solutions-oriented, and committed to continuous improvement
- Strong written and verbal communication skills, with the ability to explain technical concepts clearly.

- An understanding of, and commitment to, the College's E&D and safeguarding policies and have practical ideas for their implementation through the duties of this post.

Additional Information:

Working Arrangements

A routine start and finish time between 08.00-18.00 is required and will be arranged directly with line manager.

All staff with Group responsibility are expected to work on all sites. Under exceptional circumstances e.g. alterations in the College's pattern of working/changes in pattern of demand, the hours of attendance may be varied after consultation with the member of staff concerned. The nature of the role may demand unplanned extended hours. Unless extensive, this will be reimbursed through TOIL in the first instance.

This job description will be reviewed annually to ensure that it is an active description of the responsibilities and duties of the individual post holder and that these responsibilities and duties consistently match the needs of the College.