More House School

Job Description: Network and Security Engineer (NSOC Engineer)

Duties and Responsibilities:

Network Infrastructure

- Advise on the design, configuration, and maintenance of the School's wired and wireless network infrastructure
- Manage switching, routing, VLANs, and network segmentation
- Ensure high availability and performance of all network services
- Oversee internet connectivity, filtering, and bandwidth optimisation
- Maintain accurate network documentation, diagrams, and configurations

Cyber Security & Risk Management

- Implement and manage cyber security controls across all systems and networks
- Monitor security posture and respond to threats, vulnerabilities, and incidents
- Lead on vulnerability scanning, patching strategies, and remediation
- Support development and enforcement of IT and cyber security policies
- Conduct regular security reviews, audits, and risk assessments
- Act as the School's technical lead for cyber security operations
- Advise the Head of IT Services on risks, threats, and mitigation strategies

Firewall & Perimeter Security

- Configure and manage firewalls, intrusion detection/prevention systems, and secure gateways
- Maintain network access controls, VPNs, and remote access solutions
- Ensure appropriate segmentation of sensitive systems and data

Helpdesk Management & Service Reporting

- Manage day-to-day IT helpdesk operations, ensuring that tickets are triaged, assigned an owner, progressed, and escalated where necessary. Ensure that issues are resolved effectively.
- Oversee the full ticket lifecycle, including logging, categorisation, communication, resolution, and closure.
- Monitor queues, follow up outstanding issues, and ensure timely user updates.
- Produce monthly helpdesk reports covering volumes, trends, risks, recurring issues, and improvement actions.
- Use helpdesk data to improve service delivery, planning, and the user experience.

Identity & Access Management

- Support secure authentication systems, including Microsoft Entra ID (Azure AD)
- Implement and maintain MFA, Conditional Access, and zero-trust principles
- Ensure least-privilege access across systems and services

Monitoring & Incident Response

- Configure and maintain monitoring tools (e.g., Zabbix or equivalent)
- Investigate and respond to security alerts and incidents
- Act as the technical lead during cyber incidents and major outages. Lead the technical response to these events.
- Produce post-incident reports and recommend improvements
- Participate in incident response planning, testing, and real-time resolution
- Maintain logs and evidence for audit, safeguarding, and compliance purposes

Microsoft 365 & Cloud Security

- Manage and optimise Microsoft 365 security features (Defender, Intune, etc.)
- Monitor and respond to cloud-based threats and anomalies
- Ensure secure configuration of cloud services and integrations

Collaboration & Support

- Work closely with the Systems & Database Administrator and wider IT team
- Provide escalated support for complex network or security issues
- Contribute to IT projects, including infrastructure upgrades and new deployments
- Support staff awareness and training around cyber security risks and best practice

Safeguarding & Compliance

- Ensure all systems and controls align with safeguarding and data protection requirements (e.g. GDPR)
- Support safe use of technology across the School community
- Support compliance with cyber security frameworks and standards (e.g. Cyber Essentials / Cyber Essentials Plus)
- Maintain professional awareness of emerging threats, vulnerabilities, and best practice
- Participate in planned maintenance and occasional out-of-hours work when required

Apart from the duties summarised in this job description, we retain the right to include other reasonable duties which are part of, and incidental to, this type of work.

General Responsibilities:

- To treat all pupils, colleagues, parents and stakeholders in accordance with the School's values of Kindness, Spirit and Responsibility

- To ensure that all activities are undertaken in accordance with Health and Safety provisions
- To help ensure the tidiness, the monitoring and safe storage of all equipment used in the department
- Attendance at INSET training days and other formal out of School functions, including Founders' Day. You will also be required to attend regular update training in Safeguarding, and other subjects relevant to your role
- To maintain appropriate records, and complete all administrative tasks associated with the role in a timely and accurate manner

The post holder's responsibility for promoting and safeguarding the welfare of children and young persons for whom s/he is responsible, or with whom s/he comes into contact will be to adhere to and ensure compliance with the school's Safeguarding Policy Statement at all times. If in the course of carrying out the duties of the post, the post holder becomes aware of any actual or potential risks to the safety or welfare of children in the school, s/he must report any concerns to the School's Designated Safeguarding Lead (DSL) or deputy DSLs, or to the Headmaster.

This job description is due to be reviewed by 1st September 2027