

Job Description: Digital Services Manager

Grade: G10 – G11

Reports to: Chief Operating Officer

PURPOSE OF THE ROLE

The Digital Services Manager is the operational leader responsible for the delivery, security, resilience and continual improvement of all aspects of Voyage Education Partnership's digital infrastructure, technology services and cyber security arrangements.

The postholder provides leadership for both technical operations and customer-focused service delivery across the Trust, ensuring digital systems are secure, reliable, resilient and aligned to educational and organisational priorities.

The role is responsible for the management and development of the Trust's Microsoft cloud-first technology environment, including Microsoft 365, Azure, Entra ID, Intune, Defender, collaboration platforms, networks, infrastructure and end-user computing services. The postholder will lead cyber security, disaster recovery, service management, supplier performance, digital transformation and infrastructure modernisation programmes.

Working closely with the Chief Operating Officer, Executive Team and school leaders, the Digital Services Manager will ensure technology enables high-quality teaching, learning and business operations whilst maintaining compliance, safeguarding data, managing risk and supporting the Trust's long-term strategic objectives. The role has overall operational responsibility for the Trust's digital service delivery, technology infrastructure, cyber resilience and business continuity capabilities.

MAIN RESPONSIBILITIES, TASKS & DUTIES

Leadership and Governance

- Lead the operational delivery of all aspects of the Trust's digital infrastructure, technology services and cyber security arrangements.
- Develop and implement the Trust's digital strategy, ensuring technology supports teaching, learning and business operations whilst delivering value for money.
- Provide expert advice and assurance to the Chief Operating Officer, Executive Team, Trustees and school leaders on digital services, cyber security, infrastructure and emerging technologies.
- Maintain technology governance, standards, policies and procedures to ensure digital services remain secure, compliant and fit for purpose.
- Lead the development of a Microsoft cloud-first technology roadmap that supports organisational resilience, scalability and continuous improvement.

Digital Infrastructure and Technical Operations

- Lead the management, development and continual improvement of the Trust's digital infrastructure, including Microsoft 365, Azure, Entra ID, Intune, Defender, networking, telephony, connectivity and remaining on-premises systems.
- Ensure all infrastructure services are secure, resilient, appropriately monitored and aligned to agreed service levels.
- Oversee the lifecycle management of digital infrastructure, hardware, software, cloud services, licences and technology assets.

- Lead infrastructure modernisation programmes and the planned reduction of unnecessary legacy and on-premises systems.
- Maintain robust system monitoring, performance management and capacity planning arrangements.

IT Service Delivery and Customer Experience

- Lead the Trust's IT Service Desk and field support functions, ensuring the delivery of high-quality, customer-focused services to all academies and central teams.
- Establish and manage effective service management processes including incident, request, change, problem, asset and configuration management.
- Monitor service performance, customer satisfaction and service level compliance, implementing improvement plans where necessary.
- Oversee the management of major incidents, service disruptions and critical operational issues.
- Promote a culture of customer excellence, accountability and continuous improvement across the Digital Services Team.

Cyber Security and Information Protection

- Act as the Trust's operational lead for cyber security, implementing a defence-in-depth and Zero Trust approach across all systems, services and platforms.
- Lead the administration and continual enhancement of the Trust's cyber security controls, including Microsoft Defender, Entra security features, endpoint security, email protection and threat monitoring capabilities.
- Ensure robust identity and access management arrangements, including multifactor authentication, privileged access controls and role-based permissions.
- Lead vulnerability management, security assurance activities, system hardening and cyber risk reduction programmes.
- Coordinate the technical response to cyber incidents and data security events, supporting recovery, investigation and post-incident improvement activity.
- Promote cyber awareness and security culture across the Trust through training, communication and engagement initiatives.

Procurement, Suppliers and Financial Management

- Lead the procurement of digital services, infrastructure, software and technology solutions in accordance with Trust policies and procedures.
- Manage supplier relationships, contracts, performance reviews and service delivery arrangements.
- Undertake technology due diligence and cyber security assurance for third-party suppliers and service providers.
- Manage delegated budgets and contribute to business cases, investment proposals and technology planning activities.
- Ensure effective software licensing, subscription and asset management arrangements are maintained.

Projects and Digital Transformation

- Lead and deliver Trust-wide digital transformation and infrastructure projects.
- Evaluate emerging technologies and identify opportunities to improve efficiency, resilience, collaboration and educational outcomes.
- Ensure projects are delivered in accordance with agreed scope, quality, budget and timescales.
- Promote the effective adoption and governance of Microsoft technologies, including Microsoft 365, Teams, SharePoint, OneDrive, Power Platform, Intune, Entra ID, Azure and approved AI technologies.

- Drive innovation whilst ensuring security, compliance, risk management and operational sustainability remain central to decision making.

CREATIVITY AND INNOVATION

The postholder will provide leadership for innovation and continuous improvement across the Trust's digital infrastructure and technology services. They will identify opportunities to enhance operational efficiency, service quality, cyber resilience and educational outcomes through the effective use of Microsoft cloud technologies, automation, artificial intelligence and emerging digital solutions.

The postholder will work collaboratively with leaders across the Trust to develop and implement innovative, secure and sustainable technology strategies that support organisational growth, resilience and transformation.

CONTACTS AND RELATIONSHIPS

The postholder will be a member of the Trust's Operations and Finance Management Team and will lead the Digital Services Team. They will work closely with the Chief Operating Officer, Executive Team, Trustees, Headteachers and operational leaders to ensure the effective delivery of digital infrastructure, technology services, cyber security and digital transformation initiatives across the Trust.

The role requires regular engagement with staff, pupils, suppliers, managed service providers, regulators and external partners, acting as the Trust's lead professional for digital services, cyber resilience and technology operations.

DECISIONS

Discretion

The postholder operates with a high degree of professional autonomy and is expected to make informed operational, technical and service delivery decisions across all aspects of the Trust's digital infrastructure, technology services and cyber security arrangements. Decisions will frequently require the balancing of service quality, cyber risk, resilience, compliance, user requirements and value for money.

The postholder is authorised to:

- Make day-to-day operational decisions relating to the management, maintenance, security and development of the Trust's digital infrastructure and technology services.
- Determine technical solutions, infrastructure standards, service delivery methods and deployment approaches within approved policies, budgets and strategic objectives.
- Lead the operational response to major service outages, cyber security incidents and infrastructure failures, including the temporary restriction, isolation or withdrawal of systems and services where necessary to protect Trust operations, users or data.
- Approve routine changes to systems, cloud services, infrastructure and service delivery arrangements in accordance with established change management procedures.
- Manage suppliers, contracts and delegated budgets within approved limits.
- Exercise professional judgement where procedures may not provide a definitive solution and where competing operational priorities must be balanced.

Consequences

Decisions taken by the postholder directly impact the availability, security, resilience and effectiveness of digital services across Voyage Education Partnership. Poor decision making may result in disruption to teaching and learning, safeguarding systems, statutory obligations, business operations, data protection compliance, cyber security posture and the reputation of the Trust.

KNOWLEDGE AND SKILLS

Essential

- Proven experience leading digital services, infrastructure operations and technology service delivery within a complex multi-site organisation.
- Strong leadership and management skills, including the ability to lead technical teams, manage performance and drive continuous service improvement.
- Significant experience managing Microsoft cloud technologies, including Microsoft 365, Entra ID, Intune, Exchange Online, SharePoint Online, OneDrive and Microsoft Teams.
- Strong understanding of Microsoft cyber security technologies including Microsoft Defender, Conditional Access, Multifactor Authentication, Identity Protection and security monitoring capabilities.
- Experience of administering and supporting Azure cloud services and hybrid identity environments.
- Experience managing Windows 11 endpoint environments through modern device management platforms, including Intune and associated endpoint security controls.
- Strong working knowledge of Active Directory, Group Policy, DNS, DHCP, TCP/IP, routing, switching and network services.
- Experience managing enterprise wireless and network infrastructure, including Aruba switching and wireless networking solutions.
- Experience of managing and supporting Fortinet technologies, including FortiGate firewalls, security policies, VPN services and network protection controls.
- Experience of supporting and optimising ManageEngine solutions, including service management, device management, monitoring and asset management platforms.
- Strong understanding of cyber security principles, risk management, vulnerability management, incident response and organisational resilience.
- Experience developing and testing backup, disaster recovery and cyber recovery arrangements across both cloud and on-premises environments.
- Experience of managing technology suppliers, support contracts, service level agreements and digital procurement activities.
- Ability to assess technical and cyber risks and present complex information clearly to non-technical audiences.
- Ability to lead digital transformation projects and technology modernisation programmes from concept through to implementation.
- Knowledge of UK GDPR, Data Protection legislation, safeguarding requirements and DfE Digital and Technology Standards for schools and trusts.
- Full UK driving licence and access to appropriate transport.

Desirable

- Experience of implementing or maintaining a Microsoft cloud-first operating model.
- Experience of Zero Trust security architectures and modern identity management approaches.
- Knowledge of Microsoft Power Platform, Power BI and automation technologies.
- Experience of supporting artificial intelligence and emerging digital technologies within an education environment.
- Experience of developing operational dashboards, reporting solutions and data-driven service improvements.
- Understanding of education sector management information systems and cloud-integrated education platforms.
- Experience of operating within a Multi-Academy Trust or educational environment.

Qualifications

One or more of the following qualifications would be desirable:

- Microsoft Certified (Azure, Microsoft 365, Security, Identity, Endpoint Administrator or equivalent).
- ITIL Foundation or higher qualification.
- Cyber security qualification such as Security+, SC-900, SC-200, CISSP, CISM or equivalent.
- Networking qualification such as CCNA, Aruba Certified Professional, Network+ or equivalent.
- Project management qualification such as PRINCE2, AgilePM or equivalent.

WORK ENVIRONMENT

Work Demands

The postholder operates within a dynamic and fast-paced environment, balancing strategic development, operational service delivery, cyber security, digital transformation and incident management activities across the Trust.

The role requires the ability to manage competing priorities, respond effectively to emerging issues and make informed decisions in situations where service continuity, cyber resilience, safeguarding, compliance and organisational performance may be impacted. Periods of increased demand may occur during major projects, critical incidents, cyber security events, infrastructure changes and business continuity activations.

Physical Demands

The role is primarily office based; however, the postholder will be required to visit academies, technical facilities and supplier locations across the Trust. Occasional physical activity may be required in connection with the installation, inspection or movement of technology equipment, network infrastructure and associated resources.

Working Conditions

The postholder will work across multiple educational and corporate environments within the Trust and will be expected to develop a detailed understanding of local operational requirements.

Voyage Education Partnership supports agile and flexible working. Subject to operational requirements, service delivery needs and attendance at key meetings, hybrid working arrangements may be available. The postholder will be expected to maintain an effective presence across Trust sites and to attend locations as required to support service delivery, project implementation, leadership responsibilities and incident response activities.

Occasional out-of-hours working may be required to support infrastructure changes, system upgrades, major incidents, business continuity arrangements and cyber security response activities.

Work Context

The role requires regular engagement with senior leaders, trustees, staff, pupils, suppliers, regulators and external partners. The postholder will frequently be required to communicate complex technical information to non-technical audiences and provide assurance, advice and recommendations on matters relating to digital services, cyber security and organisational resilience.

The postholder will operate in an environment where technology services are critical to educational delivery, safeguarding and Trust operations. As a result, they must be capable of remaining professional, resilient and solution-focused when managing service disruption, cyber incidents, competing priorities and organisational change.

GENERAL

Other Duties

The duties and responsibilities in this job description are not exhaustive. The postholder may be required to undertake other duties that may be required from time to time within the general scope of the post.

Any such duties should not substantially change the general character of the post. Duties and responsibilities outside of the general scope of this grade of post will be with the consent of the postholder.

Equal Opportunities

Voyage Education Partnership is committed to creating an inclusive and diverse working environment where everyone is treated with dignity, fairness and respect. We recognise that diversity of backgrounds, experiences, perspectives and ideas strengthens our organisation and enhances outcomes for our pupils, staff and communities.

The postholder is expected to actively promote equality, diversity and inclusion in all aspects of their work, ensuring that decisions, policies, services and relationships are free from discrimination and support equitable opportunities for all. They will contribute to a culture where every individual feels valued, respected and able to reach their full potential regardless of age, disability, gender reassignment, marriage or civil partnership status, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

The postholder will demonstrate inclusive leadership, challenge inappropriate behaviour where it occurs and support the Trust's commitment to fostering a welcoming, respectful and supportive environment for pupils, colleagues, families and stakeholders.

Health and Safety

The postholder is expected to demonstrate visible and positive leadership in relation to health, safety and wellbeing, promoting a culture in which everyone takes personal responsibility for working safely and supporting others to do the same.

The postholder will actively contribute to the continual improvement of health and safety performance by identifying opportunities to reduce risk, encouraging open reporting and learning, and ensuring that health, safety and wellbeing considerations are embedded within decision-making, planning and operational activities.

The postholder is responsible for complying with all Trust health and safety policies, procedures and safe systems of work, and for ensuring that any risks, incidents, near misses or concerns are reported and addressed appropriately. They will support the Trust's commitment to creating a proactive safety culture where learning, wellbeing and continuous improvement are valued and encouraged.

As a leader within the Trust, the postholder will be expected to act as a positive role model, championing high standards of health, safety and wellbeing and fostering an environment where people feel confident to speak up, learn from experience and contribute to a safe and supportive workplace.

Safeguarding

Voyage Education Partnership is committed to safeguarding and promoting the welfare of children and young people and expects all employees, volunteers and partners to share this commitment. Safeguarding is everyone's responsibility and is fundamental to the Trust's culture, values and decision-making.

The postholder will be expected to actively support and promote the Trust's safeguarding culture, ensuring that the safety, wellbeing and best interests of children and young people remain a priority in all aspects of their work. They will comply with all safeguarding and child protection policies, procedures and statutory

guidance, including the requirement to maintain appropriate professional boundaries and report concerns promptly and appropriately.

As a leader, the postholder will be expected to demonstrate visible commitment to safeguarding, ensuring that digital services, technology systems and operational practices support the protection of children, staff and Trust communities. This includes promoting safe and responsible use of technology, maintaining appropriate cyber security and information protection controls, and contributing to a culture in which concerns are taken seriously and acted upon without delay.

The postholder will undertake all required safeguarding training and will actively contribute to creating an environment where children, young people and vulnerable individuals feel safe, supported, respected and able to thrive. Through their leadership, they will help ensure that safeguarding remains embedded within the culture, systems and day-to-day practices of the Trust.

Reviewed August 2026