Job Description

Job Title:	IT Manager
Reports to:	Deputy CEO & Director of Quality and Support Services
Based at:	The Carr Fenton Foundation
Hours of work:	37 hours per week
Annual Leave:	45 days including 8 bank holidays
Salary:	A49 to A51

Role

The IT Manager is responsible for the leadership, management and effective delivery of IT services across the Foundation, ensuring systems are secure, reliable and effectively support educational, operational and strategic needs.

The role will lead the technology contribution to the Foundation's digital transformation, working with senior leaders and service leads to identify where technology can improve accessibility, service quality, efficiency, information use and user experience.

The postholder will develop and maintain the IT strategy and five-year technology roadmap, lead cybersecurity and service governance, manage budgets and suppliers, oversee continuity and recovery arrangements and provide formal line management for the Team. The role will provide assurance on risk, compliance, performance and investment while enabling safe innovation and sustainable technology planning.

Duties and Responsibilities

By nature of the responsibility, the following list is not exhaustive but provides a guide to the main requirements of the role. The IT Manager must be willing, flexible and prepared to carry out reasonable tasks consistent with the level and purpose of the post.

Safeguarding
All staff have a responsibility and duty of care to safeguard and promote the welfare of pupils and other people who use Foundation services. Staff must be aware of the systems which support safeguarding and must act in accordance with the Foundation Safeguarding and Child Protection Policy and Code of Conduct.

Service Delivery and Operational Leadership

- Lead and manage day-to-day IT operations and service delivery across the Foundation.
- Set service standards, priorities, escalation arrangements and performance measures.
- Ensure effective incident, problem, request and change management, including major-incident oversight.
- Use service data, user feedback, risk information and root-cause analysis to drive improvement.
- Ensure users receive professional, responsive and accessible support.

IT Strategy and Five-Year Technology Roadmap

- Develop, maintain and deliver the IT strategy and a prioritised five-year technology roadmap.
- Ensure accurate and up-to-date registers are maintained for infrastructure, systems, software applications, information assets, licences and associated support arrangements.
- Translate the Foundation's strategic priorities into a coordinated programme of digital improvement and technology-enabled change.
- Work with service leads to identify and prioritise opportunities for process improvement, digital integration, automation and improved use of data.
- Align technology planning with Foundation priorities, service needs, accessibility, sustainability and value for money.
- Provide clear options, business cases and recommendations for investment and lifecycle replacement.
- Monitor emerging technologies and support proportionate, secure and evidence-based innovation.

IT Infrastructure and Technical Operations

- Oversee the operation, maintenance and performance of servers, networks, cloud systems and end-user environments.
- Ensure high availability, resilience and reliability of systems and services.
- Oversee infrastructure & core systems, currently including: Microsoft 365, Entra ID, Intune, Exchange and hybrid environments.
- Ensure controlled deployment, configuration and lifecycle management of devices and infrastructure.

Networks, Firewall, Printing and Telecommunications

- Hold overall responsibility and accountability for the Foundation's network infrastructure, including switches, routers, VLANs, network segmentation, wireless

access points, firewalls, internet connectivity, security, performance, capacity, coverage and resilience.
- Own governance and effective operation of the Smoothwall firewall and web-filtering arrangements.
- Work closely with safeguarding leads and ensure appropriate filtering and monitoring arrangements are implemented, reviewed and evidenced in line with statutory safeguarding requirements.
- Own the Papercut print-management service, including policy, performance, licensing and improvement.
- Oversee telephony, mobile-device management and relevant hosted communications services.
- Ensure network monitoring, maintenance, security, performance and approved change are effectively managed, retaining overall accountability where technical activities are delegated to the IT Engineer or other authorised providers.

Cybersecurity, Compliance and Risk

- Lead IT security governance, operational security improvement and technology risk management.
- Conduct Cyber risk assessments, reviews and create and maintain the organisation's Cyber Response Plan, coordinating organisational responses to significant cyber incidents.
- Coordinate Cyber Essentials Plus compliance, evidence, remediation and audit activity.
- Maintain appropriate security policies, standards, access controls, monitoring and incident-response arrangements.
- Work in partnership with the Performance, Insights and Data Protection Officer and safeguarding leads to ensure technology services support data protection, information governance and safe technology use.
- Ensure data protection by design and by default is embedded in the procurement, design, implementation, integration, configuration, change and decommissioning of technology systems and services.
- Ensure appropriate technical input and assurance is provided for Data Protection Impact Assessments (DPIAs), new systems, significant system changes and relevant supplier assessments.
- Ensure suspected personal-data breaches are technically contained, investigated and escalated promptly through the Foundation's established data-protection and incident-management procedures.
- Maintain and report the IT risk register, escalating material risks and control failures.

Backup, Disaster Recovery and Business Continuity

- Hold overall responsibility and accountability for backup and recovery arrangements covering servers, infrastructure, Microsoft 365 data and other critical cloud services.
- Ensure backups are appropriately monitored, failures and exceptions are addressed, restorations are completed when required, and restoration tests and recovery exercises are completed, evidenced and reviewed.
- Maintain IT disaster-recovery and business-continuity plans aligned with organisational arrangements and service priorities.
- Ensure recovery procedures, responsibilities, dependencies and escalation routes are documented and current.
- Retain overall accountability for backup and recovery arrangements where monitoring, testing, restoration or other technical activities are delegated to the IT Engineer or an external provider.

Systems and Applications Management

- Oversee administration, performance and lifecycle management of business-critical applications and integrations.
- Ensure appropriate access, licensing, support, monitoring and supplier escalation arrangements.
- Evaluate technical compatibility, security and operational impact of proposed systems and changes.
-

Supplier Management, Procurement and Finance

- Plan and manage IT budgets, forecasts, renewals and investment requirements.
- Work in partnership with the Contracts and Procurement Manager to procure IT goods and services in line with Foundation requirements.
- Manage third-party providers, contractors, consultants and relevant specialist trades, including electricians.
- Monitor supplier performance, service levels, risks, contract obligations and value for money.

Projects, Change and Lifecycle Management

- Lead infrastructure upgrades, platform changes and technology projects from initiation to handover and benefits review.
- Ensure technology projects include clear service outcomes, user requirements, adoption arrangements and proportionate benefits evaluation, rather than being treated solely as technical implementations.
- Ensure appropriate governance, risk assessment, testing, change control, communications and documentation.
- Maintain controlled lifecycle plans for devices, infrastructure, applications, licenses and support contracts.

Team Leadership and Workforce Development

- Line manage the IT Team, ensuring clear objectives, supervision, workload management and accountability.
- Set priorities and working arrangements across the IT team.
- Coordinate technical guidance and coaching provided by experienced team members.
- Build capability through coaching, training, succession planning and knowledge transfer.
- Maintain appropriate separation of duties, delegated authority and resilient cover arrangements.

Reporting and Assurance

- Provide clear reports to senior leaders and governance groups on service performance, risk, cybersecurity, compliance, projects, budgets and roadmap delivery.
- Maintain accurate documentation, inventories, licenses, contracts, diagrams and operational procedures.
- Coordinate responses to audits, reviews and assurance activity, ensuring agreed actions are completed and evidenced.

Personal Profile and Skills

The IT Manager will be a strategically minded and operationally credible leader, able to translate organisational priorities into secure, resilient and affordable technology services. They will combine strong technical understanding with service leadership, risk management, financial control and clear communication.

The postholder will provide confident assurance, make evidence-based recommendations and create the conditions in which the IT team can deliver consistently while developing capability for future needs.

Skills Overview

- IT Leadership — sets direction and assures reliable, customer-focused service delivery.
- Strategy and Roadmapping — converts organisational priorities into a deliverable five-year technology plan.
- Cybersecurity and Risk — leads governance, Cyber Essentials Plus activity, incident readiness and remediation.
- Resilience — holds overall accountability for backup and recovery arrangements and assures restoration, disaster recovery and business continuity.
- Infrastructure Governance — holds overall accountability for network infrastructure and oversees servers, cloud, identity, firewall, filtering and print platforms.

- Commercial Management — controls budgets, procurement, suppliers, contracts and value for money.
- People Leadership — line manages the full IT team and develops capability, accountability and succession.
- Senior Reporting — communicates performance, options, risks and investment needs clearly.

Training
The IT Manager may, from time to time, be required to undertake training relevant to the key objectives and responsibilities of the Foundation. Mandatory training requirements must be completed within the required timescales.

Working Relationships
The IT Manager has a day-to-day working relationship with colleagues across Foundation services and is required to cooperate fully with staff, managers and relevant external providers. A strong customer-service focus is essential.

Hours of Work
Working hours are 8.00am to 4.00pm Monday to Thursday and 8.00am to 3.30pm Friday, 37 hours in total.

The postholder may occasionally be required to work outside normal hours to support planned maintenance, projects or urgent service restoration, subject to the Foundation's arrangements. Weekend work and work outside of normal hours would be by prior arrangement and will attract time off in lieu or overtime payment.

Person Specification

The specific qualifications, experience, skills and values that are required for the role are outlined below.

Criteria	Essential =(E) Desirable =(D)
Qualifications	
Relevant degree, Level 5 or above IT qualification, or equivalent senior professional experience	E
Relevant certification in Microsoft, cybersecurity, networking, cloud or IT service management	D
Leadership or management qualification	D
Experience and Knowledge	
Significant experience leading an IT service, infrastructure function or equivalent multidisciplinary technology environment	E
Experience leading or enabling digital transformation, technology-enabled service improvement or significant organisational change	E
Experience developing IT strategy, roadmaps, service plans and investment proposals	E
Experience managing cybersecurity risk, security controls, incident response and audit activity	E
Experience overseeing and holding accountability for network infrastructure, servers, Microsoft 365, identity, endpoint management and business applications	E
Experience managing budgets, procurement, suppliers and contracts	E
Experience leading infrastructure projects, organisational change and lifecycle planning	E
Experience line managing and developing technical staff and managing workloads	E
Knowledge of Cyber Essentials Plus, data protection, safeguarding considerations and relevant technology standards	E
Experience in an education, care, charity or similarly regulated environment	D
Skills and Abilities	
Ability to provide strategic leadership while retaining effective operational oversight	E
Ability to translate organisational and service priorities into realistic digital solutions, implementation plans and measurable benefits	E
Ability to interpret service, financial, security and risk information and provide clear assurance	E
Strong programme, project, change and prioritisation skills	E
Ability to produce clear business cases and reports for senior leadership and boards	E
Strong negotiation, supplier-management and stakeholder-influencing skills	E
Ability to lead effectively during major incidents and periods of significant change	E

Ability to balance security, accessibility, service quality, affordability and innovation	E
Behavioural, Values and Ethos	
Flexible and collaborative approach, with the ability to work across teams and provide responsive support	E
Commitment to safeguarding and promoting a safe environment for children, young people, adults and staff	E
Commitment to the Foundation and to promoting equality, diversity and inclusion	E
Professional integrity and discretion when handling confidential or sensitive information	E