Job Description

The school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Role: Senior infrastructure and cloud engineer

Reporting to: Head of IT Services

Job family: Operations and professional services

Summary role:
The Senior Infrastructure and Cloud Engineer is responsible to the Head of IT Services. This role focuses on the school’s transition to cloud infrastructure. The Engineer supports applications, ensures security, and leads projects to modernise systems, including virtual infrastructure, CCTV, and MDM platforms.

Hours/weeks of work
This role is full time; some out of hours work will be required as per business needs.

Key Tasks:
1) Manage and support Microsoft 365, Azure, SharePoint, Teams, and related platforms.
2) Maintain and troubleshoot networking systems, firewalls, and wireless infrastructure.
3) Lead the transition to cloud infrastructure, ensuring system security and privacy.
4) Manage projects involving systems improvement, including CCTV and MDM platforms.
5) Provide technical expertise for the design and implementation of new systems.

Technical strategy

- **IT strategy projects**: Execute projects aligned with the school's technical roadmap and strategic IT plan, utilising the latest technologies to support and enhance the school’s operational and educational objectives.
- **Emerging technologies**: Keep abreast of developments in IT to identify and recommend suitable new technologies, systems, or processes that enhance the school’s technical capabilities.
- **Change management**: Follow and abide by the schools change management processes for IT systems, ensuring that updates, upgrades, and migrations are meticulously planned and documented.

General responsibilities and accountabilities:

- **Network and infrastructure management**: Configure and manage the core IT network, including servers, cloud solutions, and internet connectivity to ensure maximum uptime, resilience, and speed to vendor and industry best practices.
- **Cybersecurity**: Develop and enforce a robust cybersecurity framework. Ensure the schools’ systems are maintain and managed to NCSC best practices. Monitor for and mitigate threats, ensuring compliance with data protection standards and best practices.
- **System architecture**: Working with the Head of IT Services and the schools trusted partners, design and implement IT architecture and roadmaps that align with both current and future needs of the school.

- **Backup and disaster recovery**: Develop and maintain a robust backup best practice and disaster recovery plans, ensuring that all critical systems and data are backed up and recovery processes are tested and validated regularly.
- **Server and cloud management**: Manage on-premises and cloud environments, ensuring optimal performance, security, and scalability.
- **Hardware and software oversight**: Maintain hardware and software deployments, updates, and lifecycle management, including PCs, network equipment, and telephony systems as part of the rolling replacement program.
- **Customer service and service excellence:** Be a proactive member of the helpdesk, delivering and exceeding expectations and ensuring timely support in line with SLAs.
- **Asset and licensing management**: Maintain a central database of hardware and software assets, track license renewals, and ensure compliance with software licensing requirements.
- **Emerging technologies**: Keep abreast of developments in IT to identify and recommend suitable new technologies, systems, or processes that enhance the school's technical and training capabilities.
- **Change management**: Follow and abide by the schools change management processes for IT systems, ensuring that updates, upgrades, and migrations are meticulously planned and documented.

Compliance

- **Policies and documentation:** Ensure departmental documentation is accurate, current, and well-maintained across all systems. Develop, update, and distribute relevant policies to uphold excellent IT governance standards.
- **Data protection compliance**: Implement and monitor compliance with data protection legislation, coordinating with the Bursar and other stakeholders to ensure data is securely managed and appropriately accessed.
- **Safeguarding**: Collaborate with the Designated Safeguarding Lead (DSL) to monitor and report on internet and network usage, ensuring alignment with KCSIE guidance and the schools' safeguarding policies.

Safeguarding

This role will require regular interaction with pupils which equates to regulated activity with children. The post holder must at all times act with due regard to the school's child protection and safeguarding policies and procedures and the school's code of conduct.

The following duties will be deemed to be included in the duties which you may be required to perform:

- child protection
- promoting and safeguarding the welfare of children and young persons for whom you are responsible and with whom you come into contact.

General responsibilities:

- To ensure all duties are carried out in accordance with Health and Safety regulations
- To undertake any training and development for the better fulfilment of the post
- To undertake any ad hoc duties or projects as requested
- To undertake any other duties and responsibilities as determined by the Head or Bursar.

This job description contains an outline of the typical functions of the job and is not an exhaustive or comprehensive list of all responsibilities tasks and duties. The jobholder's actual responsibilities, tasks and duties might differ from those outlined in the job description and other duties commensurate with this level of responsibility may be either permanently or temporarily assigned as part of the job.

This job description is subject to review in line with the developing needs of the school.

Person Specification

Role:

	Essential	Desirable	Evidence/ Assessed By
Qualifications and training	Related technical field or equivalent work experience.	Degree and/or additional certifications, such as Cisco Certified Network Professional (CCNP) or Microsoft Certified. Cisco Certified Network Associate (CCNA) or equivalent certification	Application form, certificates.
Experience	Proven experience managing enterprise-level cloud platforms (e.g., Microsoft Azure, Microsoft 365). Extensive experience in network management, including wired and wireless infrastructure.	Experience working in educational institutions or managing complex multi-site networks.	Application form, references, interview.
Professional Values	Security-focused mindset with an emphasis on proactive risk management and privacy protection.	Commitment to optimising infrastructure for long-term sustainability and scalability.	Interview, references.
Knowledge and understanding	Strong understanding of network security principles, VPNs, and firewall configurations. Experience with Microsoft Intune and Mobile Device Management (MDM) platforms, particularly JAMF.	Familiarity with implementing Zero Trust security frameworks. It is desirable that this member of staff has a working knowledge of the following technologies: • Network management (switches, routing, firewalls, Wi-Fi, and associated servers) ○ Fortinet (FortiGate, FortiSwitch, FortiWiFi) • Sophos (Endpoint Protection, XDR and MDR) • User account management (including annual rollovers and online learning resources) • Microsoft Suite across O365 and Office Applications • Microsoft Intune • Windows 11 • Apple Hardware and Services across iPad, Apple TV and Apple Classroom • DELL Hardware (Endpoint, Servers and Storage) • Jamf • Extreme Networks WiFi	Application form, interview.

	Essential	Desirable	Evidence/ Assessed By
		• HPE Aruba (Wireless and Switching) • Salamander • Exclaimer • Veeam Backup • Impero • Barracuda Email Protection • Web-filtering solutions such as FastVue, Smoothwall or Securly • Freshdesk Helpdesk Platform • iSAMS MIS • Microsoft SQL • Windows Server • Photocopying and print management systems (Papercut) • Internal communication systems (e.g., phone systems, CCTV, ACT door entry) • Maintaining AV infrastructure such as school projectors, TVs, and digital signage and casting devices (Apple TV's, Air Server)	
Skills	Advanced troubleshooting and problem-solving skills for both networking and cloud platforms. Exceptional documentation and reporting abilities.	Experience leading infrastructure modernisation projects.	Task/test, interview.
Personal characteristics	Visionary, adaptable, and solution-oriented.	Collaborative and open to new ideas.	References, interview.

Exeter school is an equal opportunities employer and welcomes applications from any appropriately qualified person.

Exeter school is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment. All applicants should read the school's safeguarding policy before applying. Applicants must be willing to undergo child protection screening including checks with past employers and the Disclosure and Barring Service.