

IT Systems Administrator

Role Description

Position Summary

Position Title:	IT Systems Administrator
Reports To:	Director of ICT
Position Summary:	<p>This role is a dual-focus position requiring both high-level technical expertise and a deep commitment to the school's Christian mission. You will be responsible for the stability, security, and strategic evolution of the school's digital environment, ensuring that technology serves as a seamless enabler for teaching and learning.</p> <p>The ideal candidate is a proactive "hands-on" leader who can balance rigorous backend infrastructure management (servers, networks, and security) with a high-standard of front-facing user support and empathetic service delivery.</p>
Latest Revision:	January 2026
Key Relationships:	Director of ICT, IT Team, External Technology Vendors

Key Accountabilities

Application of Christian Faith	<ul style="list-style-type: none">Lead staff Bible-based devotions according to the established roster.Apply Bible-based decision-making that aligns with the school's Christian ethos, promoting a Christ-centred approach in all professional and ethical responsibilities.Actively support the school's Christian Mission, Vision, and Values through professional practice, communication, and relationships.Serve as a positive Christian role model in speech, behaviour, and lifestyle, reflecting the teachings of Jesus Christ.Committed Christian with a passion for Christian community who is actively involved in their local church	Success Measures <ul style="list-style-type: none">Decisions and actions align with Christian ethos.
Infrastructure & System Operations	<ul style="list-style-type: none">System Maintenance & Monitoring: Maintain on-premises systems (WiFi, Servers, Network Switches). Proactively monitor bandwidth, device health, and internet stability to identify and resolve blind spots before they impact the school.Lifecycle & Patch Management: Establish a rigorous software and firmware update cycle. Apply OS and application patches immediately upon release to resolve critical security vulnerabilities and maintain stability.Hardware Remediation: Manage infrastructure hardware failures, arranging rapid repairs or replacements to minimize downtime.Strategic Planning: Oversee and determine timeframes for major IT projects—including system migrations and planned outages—scheduling them during non-term time and school holidays to ensure zero disruption to the academic calendar.	<ul style="list-style-type: none">System Uptime: Maintain High availability of core services (WiFi, Servers) during school hoursMaintenance Windows: Major infrastructure upgrades or high-impact planned outages are scheduled and completed during school holidays or pre-approved windows.Patching Compliance: Critical security patches are applied when a stable release is available; non-critical updates are completed monthly according to the maintenance cycle.

Security, Safeguarding & Compliance	<ul style="list-style-type: none"> Security Auditing: Conduct regular security checks and system audits to ensure data integrity and performance (e.g., verifying SharePoint permissions, validating backups, and identifying network bottlenecks). Data Protection & Backups: Maintain and manage robust backup procedures, ensuring the "3-2-1" principle is applied to critical school data. Conduct regular restoration tests to guarantee data can be recovered quickly in the event of hardware failure or a cyber incident. Safeguarding & Web Filtering: Manage web filtering and monitoring systems to ensure a safe digital environment for students, strictly complying with child safety policies and "Duty of Care" obligations. Identity & Access Management (IAM): Oversee user administration, including the automation of account creation/removal and license assignment. Enforce strict password policies while optimizing the login experience. Policy Enforcement: Implement and uphold Acceptable Use Policies (AUP) for computer systems, ensuring all users are correctly identified and authorized on the network. 	<ul style="list-style-type: none"> Audit Readiness: Successful completion of security audits. Any "High Risk" findings (e.g., active accounts for ex-staff, open SharePoint permissions) fixed immediately. Safeguarding Efficacy: Issues with web filter hardware/software are resolved same day and escalated to vendor where necessary. Backup Integrity: Monthly "Restoration Tests" are successful, proving that data can be fully recovered in the event of a ransomware attack or hardware failure.
Education Technology & Endpoints	<ul style="list-style-type: none"> Device Management (MDM): Utilize Mobile Device Management platforms (e.g., Intune, Jamf) to deploy apps, SSL certificates, and policies across large fleets of student and staff devices (Windows, Mac, iPad, BYOD). Classroom Tech Support: Ensure the reliability of interactive displays, wireless classroom display mirroring (e.g., Vivi), and AV equipment critical for daily instruction. 	<ul style="list-style-type: none"> Device Readiness: All student and staff devices (iPads, Laptops) are imaged, updated, and ready for use on the first day of Term 1, depending on supply. Classroom Continuity: "Zero-Lesson-Lost" goal for AV; interactive displays and wireless mirroring (Vivi) have a reported downtime of less than 4 hours from the time a ticket is raised.

	<ul style="list-style-type: none"> Platform Integration: Maintain and troubleshoot access to key educational platforms (e.g., Microsoft 365, Canvas LMS) to ensure seamless availability for teaching and learning. 	<ul style="list-style-type: none"> MDM: Apps up to date, correct restrictions in place and correct apps deployed to users.
User Support, Documentation & Service Excellence	<ul style="list-style-type: none"> Service Delivery: Lead the development of a strong customer service culture, providing empathetic support to users with varying levels of technical literacy (from students to executive staff). Knowledge Management: Maintain the internal knowledge base (e.g., Service Desk Plus) and create clear, non-technical Self-Help Guides to empower users and reduce Level 1 support tickets. Process Optimization (ITIL): Continuously improve team efficiency by adopting ITIL best practices for helpdesk workflows and refining internal controls. System Documentation: Meticulously document system configurations, change logs, and disaster recovery procedures to ensure business continuity. 	<ul style="list-style-type: none"> Ticket Deflection: A measurable increase in users accessing "Self-Help" guides before submitting a ticket, resulting in fewer "How-To" queries for the team. Satisfaction Score: Maintain a high Customer Satisfaction rating on post-ticket surveys from teachers and staff. Documentation Freshness: System configurations and disaster recovery plans are reviewed and updated annually (or immediately following a major change).

Organisation Position

Director of ICT
IT Systems Administrator
No direct reports

Qualifications, Skills & Experience

Essentials

- Active Christian faith and regular attendance at a Christian Church.
- Demonstrated commitment to the Vision, Mission and Values of WCCS, including the Statement of Faith.
- Proven ability to troubleshoot effectively in the event of infrastructure failure, including network, internet and server infrastructure.
- Current Working with Children Check (WWCC) or local criminal record screening.
- The ability to explain complex technical issues to a wide audience of non-technical users is highly valued.
- Ability to prioritise multiple urgent requests
- Willingness to learn from others and pass on knowledge.
- Solid understanding of networking fundamentals (VLANs, Routing, Firewall management, and Wireless Access Points).
- Excellent interpersonal and communication skills and ability to work effectively in a team structure and independently.
- Strong hands-on experience with Windows Server (Active Directory, Group Policy, DNS/DHCP) and Virtualization (Hyper-V or VMware)

Desirables

- ITIL Foundation Certification and understanding the framework for service management.
- Industry Certifications: Microsoft (AZ-800/801), Cisco (CCNA), or CompTIA Network+/Security+.
- Experience with PowerShell, Python, Shell scripts
- Experience with API integrations
- 3-5 years experience in a Systems Administrator or Senior Desktop Support role.
- Professional experience using MDM tools (e.g., Microsoft Intune, Jamf, or Google Admin) to manage a diverse fleet of devices.
- Experience managing Microsoft 365 (Exchange, SharePoint) or Google Workspace for Education.