



Position Description

Information Technology Manager

Position Summary

The Information Technology (IT) Manager provides strategic and operational leadership for Information and Communications Technology across Marist Regional College. The role is responsible for the design, security and ongoing development of the College's IT infrastructure and systems, ensuring that they are resilient, secure, and aligned with the educational mission of the College.

Leading a team of IT support staff, the IT Manager oversees a broad range of technology encompassing endpoint management, network infrastructure, identity and access management, cyber security, and the delivery of business and learning technologies across the College, including student information, learning management, human resources, and finance systems.

Key Objectives:

- Lead and develop the IT team to deliver effective, responsive support and services across the College.
- Design, maintain, and continuously improve a secure and reliable IT infrastructure supporting approximately 1,500 devices across the College IT environment.
- Develop and implement IT security strategy, ensuring alignment with recognised frameworks and the protection of college data and systems.
- Partner with College leadership and the IT Committee to shape the strategic direction of digital technology in support of the College's educational vision.
- Manage IT vendor relationships, procurement, and lifecycle planning to ensure cost-effective and fit-for-purpose technology investments.
- Lead the ongoing migration of college systems and services toward a cloud-first environment, ensuring continuity of operations and minimal disruption to staff and students throughout the transition.
- Guide the College's approach to emerging technologies, including artificial intelligence, ensuring responsible adoption that supports educational outcomes and manages associated risk.

This position is offered as Full-Time, ongoing.

Accountability

All positions within the College are expected to uphold and promote the Mission, Vision, and Values of Marist Regional College, and to conduct all duties in a manner consistent with the Catholic ethos of the College.

The IT Manager is directly accountable for:

- The security, availability, and integrity of the College's IT infrastructure and systems
- Leadership, performance, and the on-going development of the IT support team
- IT budget management, procurement oversight, and asset lifecycle planning.
- Compliance with relevant legislation, including privacy obligations under the Privacy Act 1998 and obligations under the Australian Cyber Security Centre's Essential Eight framework
- Vendor and contract management for IT-related services and equipment
- Reporting to IT Committee and College leadership on IT strategy, risk, and performance.

Authority

The IT Manager is appointed by the Principal in consultation with the Business Manager and Deputy Principals. The IT Manager is directly accountable to the principal.

The IT Manager is **responsible for**:

- IT Support Officer(s)
- IT Support Trainee(s)

Key Relationships

<i>Internal</i>	IT Committee, College Leadership Team, Business Operations Team's
<i>External</i>	Catholic Education Tasmania (CET), and relevant external vendors and service providers

Occupational Health & Safety

This Position is classified as '**Worker**' under the Work Health & Safety Act (Tas) 2012, and the incumbent is responsible to undertake duties specified as '**Worker**' for the purpose of this Act.

In addition, all employees of MRC are required to:

- Cooperate with the College in relation to activities taken by MRC to comply with WHS legislation;
- comply with the Work Health & Safety Act (Tas) 2012 and Regulations;
- adopt work practices that support WHS programs;
- take reasonable care for their own health and safety and the health and safety of other people who may be affected by their conduct in the workplace;
- seek guidance for all new or modified work procedures;

- ensure that any hazardous conditions, near misses and injuries are reported immediately;
- participate in meetings, training and other environment, health and safety activities where required;
- not willfully place at risk the health or safety of any person in the workplace;
- not willfully or recklessly interfere with or misuse anything provided in the interest of environment health and safety or welfare.

Tasks & Responsibilities

The following tasks are indicative of the role and are not intended to be exhaustive. The Principal may vary or adjust key tasks after appropriate consultation with the IT Manager.

Infrastructure & Systems

- Design, maintain, and continuously improve the College's network infrastructure including switching, routing, wireless, firewalls, and security.
- Oversee the College's hybrid cloud and on-premises environments, ensuring integration, availability, and appropriate access controls across all platforms and services.
- Manage endpoint lifecycle across the College's device estate, including deployment, configuration, and retirement of staff and student devices.
- Oversee administration of IT hardware, software, IoT devices, and third-party platforms and services.
- Ensure software licensing compliance across all College systems and users.
- Maintain business continuity and disaster recovery capability, including backup systems and document recovery procedures.
- Configure and maintain system monitoring and alerting to ensure timely detection of and response to critical infrastructure events and ensure the IT team has clear procedures for incident escalation and resolution.

Cybersecurity & Compliance

- Assume primary responsibility for the security of the College's network, systems, and data, applying recognised frameworks and best-practice standards.
- Develop, implement, and maintain IT security policies, procedures, and controls.
- Monitor for and respond to security incidents, vulnerabilities, and threats.
- Ensure the College meets its obligations under relevant privacy legislation and applicable cybersecurity standards.
- Conduct or commission periodic risk assessments and audits of IT systems and practices.

Team Leadership

- Lead, supervise, and develop IT support staff, including day-to-day direction, workload management, and professional development.
- Foster a high-performing, service-oriented team culture within the IT function.

- Recruit IT team members and project resources as required.

Strategy, Planning & Governance

- Develop and implement IT strategies, policies, and roadmaps aligned to the College's current and future needs.
- Contribute strategically to the evolution of the College's Learning Management System, Student information System, and their integrations with other platforms.
- Ensure IT procurement and outsourcing decisions represent value for money and are aligned to the College's strategic direction.
- Liaise with both the Principal, Business Manager, and other senior stakeholders on the IT investment, risk, and operational matters.

Project Management

- Manage ICT projects across the full project lifecycle using standard project management practices.
- Define and maintain project scope, schedules, budgets, and quality targets.
- Report project status to the Principal, Business Manager, IT Committee at appropriate intervals.
- Coordinate internal and external project stakeholders to achieve defined outcomes.

Stakeholder Engagement & Professional Development

- Serve as the primary IT liaison for college leadership, staff, students, and external service providers.
- Attend and contribute to IT Committee meetings, providing strategic and operational reporting.
- Represent the College as an active member in *MITIE (Management of Information Technology in Education)* professional network.
- Maintain current knowledge of developments in educational technology, cybersecurity, and IT management practice.

Selection Criteria

Essential Requirements

1. Qualifications & Experience
 - a. A tertiary qualification in Information Technology, Computer Science, or related discipline; or equivalent demonstrated experience in a senior IT role.
 - b. Significant experience in an IT management or senior IT leadership role, ideally within an education, government, or similarly complex multi-stakeholder environment.
 - c. Demonstrated experience leading and developing a team of technical staff, including performance management, workload prioritisation, and professional development.
2. Technical Capability

- a. Demonstrated experience designing, managing, and securing enterprise-grade network infrastructure, including switching, routing, wireless, and firewalls.
- b. Experience administering hybrid cloud and on-premises environments, including identity management, directory services, student information systems, and productivity platforms.
- c. Experience managing endpoints across a mixed-platform environment, including device enrolment, configuration management, policy enforcement, software deployment, and patching, across college owned devices.
- d. Demonstrated experience applying recognised cybersecurity frameworks (such as the *ACSC E8*, *NIST CSF*, or *ISO 27001*) in an operational environment.
- e. Understanding of backup, disaster recovery, and business continuity principles and practice.
- f. Sound understanding of virtualisation and server infrastructure technologies.

3. Leadership, Communication & Governance

- a. Demonstrated ability to communicate complex technical concepts clearly and effectively to non-technical stakeholders, including senior leadership.
- b. Experience developing and managing IT budgets, procurement processes, and vendor relationships.
- c. Experience planning and delivering IT projects using structured project management approaches.
- d. Sound understanding of relevant privacy legislation, including obligations under the *Privacy Act 1998 (Cth)* and the *Notifiable Data Breaches Scheme*.
- e. Ability to develop, implement, and review IT policies, procedures, and governance frameworks.

4. Organisational Fit

- a. Commitment to ongoing professional development and currency of knowledge in a rapidly evolving field.
- b. Understanding of, and willingness to contribute to, the mission and Catholic ethos of Marist Regional College.
- c. Commitment to child safety and the wellbeing of students in all aspects of the role.

Desirable Requirements

- Relevant industry certifications in cybersecurity (such as *CompTIA Security+*, *CISSP*, *CCSP*, or *CISM*), cloud platforms (*AZ-900*, *AZ-104*, or *AWS-CCP*), or networking (*CCNA*, *JNCA*, or *VCP-NV*).
- Project management certification (such as *PMP*, *PRINCE2*, *SAFe*, or *PMBOK*-aligned qualification).
- Demonstrated experience planning or executing cloud migration projects, including the transition of on-premises systems and services to cloud-hosted platforms.
- ITIL Foundation certification or equivalent service management knowledge.
- Experience with AI governance, acceptable use policy development, or the integration of generative AI tools in an organisational setting.

- Active participation in professional networks relevant to educational technology (such as *MITIE*).
- Experience working within a Catholic or independent school environment.

Acceptance of responsibility

I confirm that I have read, understood, and accept the responsibilities, accountabilities, and expectations set out in this Position Description.

I understand that the key tasks and responsibilities of this role may be varied or adjusted by the principal following appropriate consultation, and that this Position Description will be reviewed periodically to reflect the evolving needs of the College.

I acknowledge my obligations under the *Work Health & Safety Act (Tas) 2012* and the *Work Health and Safety Regulations 2022* and commit to conducting all duties in a manner that supports the health, safety and wellbeing of myself and others.

Employee:

Name

Signature

Date