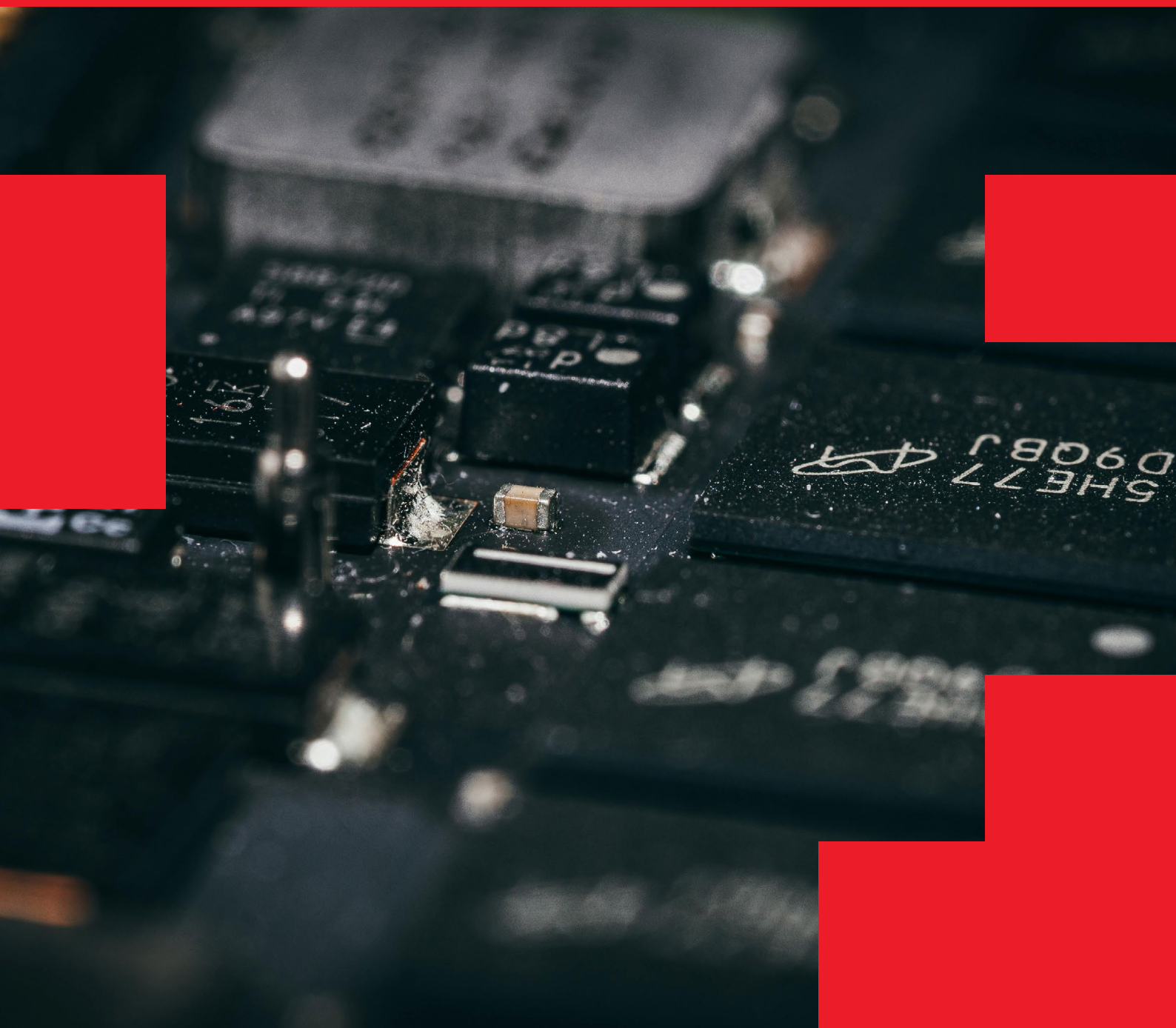
KNIGHTS

Technology Infrastructure Policy



Document Overview			
Title:	Technology Infrastructure Policy		
Document Number:	KNIGHTS_TIP_001	**Document Type:**	Policy

Version History		
Version No.	**Date**	**Description of Changes**
V1	Mar 26	Initial Document Creation

Continuous Improvement

Policies, procedures and processes are meant to be 'living' documents that need to be followed, implemented and maintained. If the procedure does not reflect the current, correct work practice please contact us on quality@knights.edu.mt

Technology Infrastructure Policy

1. Purpose

The purpose of this policy is to ensure that **Knights College** maintains a secure, reliable, and scalable technology infrastructure capable of supporting teaching, learning, administrative operations, and institutional communication. Knights College recognises that the delivery of modern education depends on digital platforms and information systems that must remain accessible, secure, and resilient.

This policy establishes the governance framework, operational standards, and security principles required to maintain the integrity, availability, and confidentiality of technology systems used by Knights College. The policy also ensures that Knights College's digital infrastructure supports the effective delivery of academic programmes while safeguarding information resources.

2. Scope

This policy applies to all technological systems and digital infrastructure used by **Knights College** to support academic delivery, administrative processes, communication, and data management. The scope includes cloud services, learning management systems, communication platforms, institutional databases, document storage systems, and other digital tools used for academic and operational activities.

This policy applies to all staff members, students, contractors, and authorised external partners who access or manage technology systems used by Knights College. The policy also applies to third-party service providers whose technology platforms or infrastructure support the operations of Knights College.

3. Definitions

For the purposes of this policy, technology infrastructure refers to the hardware, software, networks, and cloud-based systems used by **Knights College** to support teaching, learning, communication, and administrative activities.

A Learning Management System refers to the digital platform used by Knights College to deliver learning materials, manage assessments, facilitate communication between lecturers and students, and support online or blended learning activities.

Cloud infrastructure refers to externally hosted digital services accessed via the internet that support the operations of Knights College, including productivity platforms, communication tools, storage services, and other software systems.

Critical systems refer to digital systems that are essential for the delivery of educational programmes and the operation of Knights College, including learning platforms, communication systems, and institutional data repositories.

Institutional data refers to all information created, processed, stored, or transmitted by Knights College in the course of its academic, administrative, or operational activities.

4. Regulatory Compliance

This policy forms part of the Internal Quality Assurance framework of **Knights College** and supports compliance with regulatory expectations applicable to licensed education providers. Knights College is committed to maintaining technology infrastructure that supports the delivery of educational programmes in accordance with the standards and regulatory expectations established by the **Malta Further and Higher Education Authority**.

This policy also supports compliance with applicable data protection legislation and internal data protection policies governing the processing and protection of personal data.

5. Infrastructure Overview

Knights College operates a cloud-based technology infrastructure designed to support digital learning, communication, and administrative management. This infrastructure incorporates modern technology platforms that provide scalability, system resilience, and data protection.

Knights College utilises digital platforms including learning management systems, productivity and communication tools, institutional data storage systems, and other technology solutions that support the delivery of academic programmes and administrative activities. These systems are configured to ensure secure access for authorised users and reliable availability of digital learning resources.

The architecture of the technology infrastructure used by Knights College incorporates redundancy and resilience measures intended to minimise service interruptions and ensure that critical systems supporting teaching and learning activities remain accessible.

6. Governance and Responsibilities

Knights College recognises the importance of effective governance in managing technology infrastructure and ensuring that digital systems support academic delivery.

Senior management is responsible for ensuring that adequate technological resources are available to support the activities of Knights College and that infrastructure systems are maintained in accordance with institutional policies and regulatory requirements.

The IT Administrator or designated technology management function is responsible for overseeing the operational management of technology infrastructure used by Knights College. This responsibility includes maintaining system functionality, managing user access, implementing security controls, monitoring system performance, coordinating system updates, and managing backup and recovery procedures.

The quality assurance structures of Knights College oversee the effectiveness of technology infrastructure in supporting the delivery of academic programmes and ensuring that digital systems remain suitable for teaching and learning activities.

Where applicable, the Data Protection Officer ensures that systems used by Knights College comply with relevant data protection legislation and that personal data processed through institutional systems is protected appropriately.

7. Access Control

Access to technology systems used by **Knights College** is controlled through authentication mechanisms and role-based permissions. Knights College ensures that access to digital systems is granted only to authorised individuals and that user permissions correspond to the responsibilities and roles of each user.

User accounts are created for staff and students based on official enrolment or employment records at Knights College. Access permissions are periodically reviewed to ensure that users maintain appropriate levels of access to digital systems. When individuals leave Knights College or no longer require access to specific systems, their accounts are disabled or removed promptly to prevent unauthorised access.

Authentication procedures are designed to maintain system security and may include password complexity requirements and additional security measures such as multi-factor authentication where appropriate.

8. Data Security and Protection

Knights College implements appropriate technical and organisational measures to protect institutional data from unauthorised access, loss, alteration, or destruction. Security measures are designed to ensure the confidentiality, integrity, and availability of information managed by Knights College.

Technology systems incorporate safeguards such as encryption, malware protection, secure communication protocols, and monitoring tools that detect potential security threats or vulnerabilities. Systems are periodically reviewed to ensure that security protections remain effective and aligned with evolving technological risks.

All systems processing personal data must comply with applicable data protection legislation and internal data protection policies implemented by Knights College.

9. Data Backup and Recovery

Knights College maintains regular data backup procedures to ensure the protection and availability of critical institutional information. Backup processes are designed to safeguard data against accidental loss, system failures, or other disruptions that may affect the operations of Knights College.

Backup systems operate according to defined schedules and ensure that institutional data can be restored when necessary. Backup data is stored securely and protected against unauthorised access or modification.

Knights College periodically tests data restoration procedures to verify that backup systems operate effectively and that critical information can be recovered within appropriate timeframes.

10. Disaster Recovery and Business Continuity

Knights College maintains procedures designed to ensure that critical technology systems can be restored and academic activities can continue in the event of technology failures, cyber incidents, or other disruptions. Disaster recovery planning aims to minimise disruption to teaching, learning, and administrative operations.

Where system interruptions occur, Knights College will take appropriate steps to restore services and ensure that academic delivery can continue with minimal disruption. Contingency arrangements may include alternative communication channels, temporary digital platforms, or other operational adjustments that support the continuity of teaching and learning activities.

Disaster recovery procedures are reviewed periodically to ensure that they remain effective and appropriate for the technological environment of Knights College.

11. Incident Management

Knights College maintains procedures for managing technology-related incidents, including system outages, operational disruptions, and security incidents. All users are expected to report technology incidents promptly to the responsible technology management function at Knights College.

Reported incidents are investigated to determine their causes, and appropriate corrective actions are implemented to restore system functionality and prevent recurrence. Where incidents involve potential data breaches, Knights College follows applicable data protection procedures and regulatory reporting requirements.

Records of incidents are maintained to support continuous improvement of technology management practices.

12. Monitoring and Maintenance

Technology systems used by **Knights College** are monitored to ensure that they operate effectively and continue to support academic and administrative activities. Monitoring activities assist in identifying system performance issues, security alerts, and potential operational risks.

Regular maintenance activities are conducted to ensure the continued reliability of systems used by Knights College and to apply necessary software updates or security improvements. Maintenance activities are scheduled in a manner that minimises disruption to teaching and learning activities wherever possible.

13. Third-Party Technology Services

Knights College may engage external service providers to support its technology infrastructure and digital learning environment. When third-party services are used, Knights College ensures that service providers maintain appropriate security standards and comply with relevant legal and regulatory requirements.

External providers are expected to implement safeguards to protect institutional data and maintain reliable service availability. Where applicable, service agreements are established to ensure that external services meet the operational and security requirements of Knights College.

14. Acceptable Use

All users of technology systems provided by **Knights College** are required to use these systems responsibly and in accordance with institutional policies. Technology systems

are provided to support educational, research, and administrative activities, and users must ensure that their use does not compromise system security or disrupt operations.

Users are responsible for safeguarding their login credentials and ensuring that systems are not used for unauthorised or inappropriate purposes. Failure to comply with technology policies may result in disciplinary action in accordance with the procedures of Knights College.

15. Policy Review

This policy shall be reviewed **at least once every twelve (12) months** to ensure that it remains relevant, effective, and aligned with the operational needs of Knights College, technological developments, and regulatory expectations.

The policy may also be reviewed earlier where necessary due to changes in regulatory requirements, technological infrastructure, or institutional operations.