



Data Privacy and Information Management





Document Overview

Title:	Data Privacy and Information Management Policy		
Document Number:	KNIGHTS_DPIM_001	Document Type:	Policy

Version History

Version No.	Date	Description of Changes
V1	Mar26	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



Data Privacy and Information Management Policy

Knights College

1. Purpose

The purpose of this policy is to establish the institutional framework governing responsible management, protection, and lawful processing of personal data by Knights College. The institution recognises that the protection of personal information is essential to maintaining trust with students, staff, applicants, and external stakeholders and forms an important component of responsible educational governance.

This policy sets out the principles and procedures that guide how personal data is collected, processed, stored, shared, and retained by the institution during the delivery of educational programmes and administrative services. The policy ensures that personal data is handled in a manner that safeguards the rights and freedoms of individuals while supporting the operational, academic, and regulatory obligations of the institution.

Knights College is committed to ensuring full compliance with the requirements of the [General Data Protection Regulation \(EU\) 2016/679](#), the [Data Protection Act \(Chapter 586 of the Laws of Malta\)](#), and the regulatory expectations established by [the Malta Further and Higher Education Authority](#). Through this policy, the institution promotes transparency, accountability, and responsible information governance across all areas of its operations.

2. Scope and Applicability

This policy applies to all personal data processed by or on behalf of Knights College in connection with its educational, administrative, and governance activities. The policy covers all institutional operations that involve the collection, storage, use, transmission, or deletion of personal data.

The policy applies to all members of the Knights College community, including academic staff, administrative staff, students, applicants, contractors, consultants, and any third parties who process personal data on behalf of the institution. All individuals associated with the institution are required to comply with the principles and responsibilities set out in this policy when handling personal information.

The policy applies to personal data held in any format or location, including institutional databases, student information systems, learning management systems, communication platforms, cloud-based services, and physical archives or records maintained by the institution.

3. Definitions



For the purposes of this policy, personal data refers to any information relating to an identified or identifiable individual. This includes information such as names, identification numbers, location data, contact details, academic records, and any other information that can directly or indirectly identify a person.

Processing refers to any operation performed on personal data, including its collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

A data subject refers to the individual whose personal data is being processed. This may include students, staff members, applicants, alumni, or other individuals whose personal information is held by the institution.

Knights College acts as the data controller for the personal data processed in connection with its institutional activities. Where external service providers process data on behalf of the institution, those organisations act as data processors and must comply with contractual and regulatory obligations governing data protection.

Special category data refers to sensitive personal data that requires additional protection under data protection legislation. This may include information relating to health, disability status, ethnic origin, or other protected categories defined by the [General Data Protection Regulation](#).

4. Data Protection Principles

Knights College processes personal data in accordance with the principles established under the General Data Protection Regulation. Personal data must be processed lawfully, fairly, and transparently, and individuals must be informed about how their information is used.

Personal data collected by the institution is limited to information that is necessary for specified and legitimate purposes related to the delivery of educational programmes and the administration of institutional activities. The institution ensures that personal data is accurate and kept up to date where necessary and that reasonable steps are taken to correct inaccuracies when they are identified.

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected or to comply with legal and regulatory obligations. A detailed breakdown of the retention times can be found in Appendix A at the end of this document. Knights College also implements appropriate technical and organisational safeguards to protect personal data against unauthorised access, loss, misuse, or destruction.

5. Lawful Bases for Processing

Knights College processes personal data only where a lawful basis exists under the General Data Protection Regulation. In many cases, personal data is processed because it is necessary for the performance of a contractual relationship between the institution and its students or employees. This includes activities such as managing student enrolment, maintaining academic records, administering assessments, issuing qualifications, and managing employment relationships.

Personal data may also be processed where it is necessary for compliance with legal obligations imposed on the institution. Such obligations include regulatory reporting requirements, compliance with financial or taxation regulations, and responding to lawful requests from competent authorities such as the National Statistics Office

In certain circumstances, personal data may be processed on the basis of the legitimate interests of the institution. These interests may include maintaining the quality of educational provision, conducting internal quality assurance reviews, analysing institutional performance, and improving student services.

Where required, Knights College may also process personal data based on the explicit consent of the individual, particularly in relation to marketing communications or participation in promotional activities. Individuals may withdraw consent at any time.

Knights College may also process personal data for the purpose of sending marketing communications relating to its educational programmes, events, services, and institutional updates. Such communications are sent only where the individual has provided explicit consent, or where another lawful basis under the General Data Protection Regulation applies, such as an existing student or alumni relationship. Individuals may withdraw their consent to receive marketing communications at any time by using the unsubscribe mechanism provided in each communication or by contacting the Data Protection Officer. Withdrawal of consent does not affect the lawfulness of processing carried out prior to its withdrawal.

6. Special Category Data

Knights College may process special category personal data where necessary to support the welfare, accessibility, and educational needs of students or staff. This may include information relating to disabilities, health conditions, or other circumstances requiring the provision of reasonable adjustments or support services.

Such data is processed only where appropriate safeguards are in place and access is restricted to authorized personnel who require the information to fulfil their professional responsibilities. The institution ensures that such information is handled with strict confidentiality and respect for the privacy of individuals.

7. Data Collection

Knights College collects personal data through institutional processes associated with admissions, enrolment, academic administration, student services, and institutional governance. Data may be collected through application forms, enrolment documentation, academic assessments, attendance monitoring systems, surveys, correspondence, or digital interactions with institutional platforms.

Information collected may include identification details, contact information, academic records, attendance records, financial information, and other information necessary for the proper administration of educational programmes and institutional services.

Knights College may collect personal data for marketing and student recruitment purposes through voluntary interactions with its digital and physical platforms. These may include newsletter subscriptions, event registrations, submission of enquiry forms, participation in promotional campaigns, social media lead-generation forms, and interactions with the College's website and online advertising. Only personal data that is necessary for the intended communication or engagement is collected, and individuals are informed at the point of collection about the purpose for which their data will be used.

8. Data Sharing and Third-Party Processing

Knights College limits the sharing of personal data to situations where such disclosure is necessary for legitimate institutional, legal, or regulatory purposes. Personal data may be shared internally with authorized staff members who require access to the information to perform their duties.

The institution may engage external service providers to support its operations, including information technology providers, cloud infrastructure services, learning management system providers, payment processors, and professional advisers. Where such providers process personal data on behalf of Knights College, the institution enters into formal Data Processing Agreements that require the service provider to comply with applicable data protection legislation and to implement appropriate technical and organisational safeguards.

These agreements ensure that third-party processors process personal data only in accordance with the instructions of Knights College and maintain appropriate security and confidentiality obligations.

To support its marketing, communications, and student recruitment activities, Knights College may engage third-party service providers such as customer relationship management systems, email campaign platforms, digital advertising services, analytics tools, and marketing agencies. Where such providers process personal data on behalf of the College, they act as data processors and are bound by formal Data Processing Agreements that ensure compliance with applicable data protection legislation. These providers may

process personal data only in accordance with the documented instructions of Knights College and must maintain appropriate technical and organisational measures to safeguard personal information.

9. International Data Transfers

Where personal data is transferred outside the European Economic Area, Knights College ensures that appropriate safeguards are implemented in accordance with the General Data Protection Regulation. Such safeguards may include the use of Standard Contractual Clauses, adequacy decisions issued by the European Commission, or other approved mechanisms that ensure an equivalent level of protection for personal data.

The institution carefully evaluates any international data transfers and ensures that appropriate contractual and organisational measures are in place to protect the rights of individuals.

10. Data Retention

Knights College maintains a structured data retention framework to ensure that personal data is retained only for as long as necessary to fulfil legal, regulatory, and operational requirements. Academic records, including transcripts and qualification records, may be retained for extended periods to support the verification of qualifications and compliance with regulatory expectations in higher and further education.

Student enrolment records may be retained for up to forty years following the termination of the student's relationship with the institution to enable the verification of academic credentials and to respond to requests from graduates, employers, or regulatory authorities.

Other categories of personal data are retained only for periods consistent with legal obligations and institutional operational needs as described in Appendix A. When personal data is no longer required, it is securely deleted, anonymised, or destroyed.

11. Data Security and Storage

Knights College implements appropriate technical and organisational measures to ensure the security and integrity of personal data. These safeguards protect personal information against unauthorised access, accidental loss, destruction, misuse, or disclosure.

Access to systems containing personal data is restricted through secure authentication systems and role-based access controls. Staff members are required to maintain confidentiality when handling personal data and must follow institutional procedures relating to information security.

The institution also maintains secure backup procedures and disaster recovery mechanisms to ensure that institutional data can be restored in the event of system failure.

Marketing and communication platforms used by Knights College are subject to the same security expectations applied across all institutional systems processing personal data. Access to marketing tools, including email campaign systems, customer relationship management platforms, and digital advertising dashboards, is restricted to authorised staff members and controlled through secure authentication and role-based permissions. Staff with access to such systems must ensure that personal data is handled in accordance with this policy and institutional information security procedures.

12. Data Breach Management

Knights College maintains procedures for identifying, reporting, and responding to personal data breaches. Staff members who become aware of a potential breach must report the incident immediately to the Data Protection Officer or designated institutional authority.

The institution will investigate the incident and assess the risks to affected individuals. Where a breach is determined to present a risk to the rights and freedoms of individuals, the institution will notify the Information and [Data Protection Commissioner](#) within seventy-two hours of becoming aware of the breach, in accordance with the requirements of the General Data Protection Regulation.

Where necessary, affected individuals will also be informed and appropriate corrective measures will be implemented to mitigate the impact of the incident.

13. Rights of Data Subjects

Individuals whose personal data is processed by Knights College have a number of rights under the General Data Protection Regulation. These rights include the right to access personal data held about them, request the correction of inaccurate information, request the deletion of data where appropriate, and request restrictions on certain forms of processing.

Individuals may also object to certain types of processing and request the transfer of their personal data to another organisation where applicable.

Requests relating to personal data should be submitted to the Data Protection Officer.

Data Protection Contact:

Email: dataprotection@knights.edu.mt

Requests will be handled in accordance with the timeframes established under applicable legislation.

Individuals have the right to object at any time to the processing of their personal data for direct marketing purposes, including profiling that is related to such marketing. Where an individual exercises this right, Knights College will cease all marketing-related processing of their personal data without undue delay. Individuals may also request the correction or deletion of marketing data, withdraw consent, or update their communication preferences by contacting the Data Protection Officer or using the mechanisms provided within marketing communications.

14. Data Protection Officer

Knights College appoints a Data Protection Officer responsible for overseeing compliance with data protection legislation and institutional policies relating to the management of personal information. The Data Protection Officer provides guidance to staff, monitors institutional compliance, and serves as the contact point for supervisory authorities and individuals whose personal data is processed by the institution.

The Data Protection Officer operates independently and reports to senior management to ensure that data protection considerations are appropriately integrated into institutional governance and decision-making processes.

15. Data Protection Impact Assessments

Where processing activities are likely to result in a high risk to the rights and freedoms of individuals, Knights College conducts Data Protection Impact Assessments. These assessments evaluate the potential privacy risks associated with proposed processing activities and identify appropriate safeguards to mitigate those risks.

The Data Protection Officer may be consulted during the preparation of such assessments, and where required the institution may consult the supervisory authority prior to initiating certain high-risk processing activities.

16. Staff Responsibilities and Training

All staff members who process personal data as part of their professional responsibilities must comply with this policy and applicable data protection legislation. Staff must ensure that personal data is handled securely, confidentially, and only for legitimate institutional purposes.

Knights College provides periodic data protection awareness training and guidance to ensure that staff understand their responsibilities in relation to information security and privacy protection.

Failure to comply with data protection obligations may result in disciplinary action in accordance with institutional procedures.

17. Complaints and Supervisory Authority

Individuals who believe that their personal data has been processed in a manner that does not comply with applicable legislation may raise their concerns with Knights College in the first instance.

If an individual is not satisfied with the response provided by the institution, they may lodge a complaint with the **Information and Data Protection Commissioner (IDPC), Malta**, which is the national supervisory authority responsible for enforcing data protection legislation.

Knights College cooperates fully with the supervisory authority in the exercise of its regulatory functions.

Appendix A – Data Retention Schedule (Summary)

Data Category	Retention Period
Student transcripts and qualifications	Permanent
Student enrolment records	Up to 40 years
Admissions records	10 years
Financial records	10 years
Employment records	10 years after termination
Marketing data	Until consent withdrawn