Data Protection Policy

Updated June 2025.

1. Introduction

Since 25 May 2018, the law regarding data protection, the rights of data subjects regarding their privacy and the responsibilities of organisations to uphold these rights have been strengthened. This policy provides the steps that can help an efficient development of the St. Julian's School community culture, processes and documentation required to be compliant with the strengthened legislation and effectively manage the risks associated. These steps will enable St. Julian's School to identify and monitor the use of personal data, undertake the necessary processes for auditing and assessing risk and assist with compiling policies to ensure compliance.

2. Basic concepts of the GDPR

2.1 What is Personal Data?

Personal Data is any information, including documents, video footage or genetic material, that relates to an identified or identifiable natural person ('data subject') directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2 Special category of Personal Data

There is a subset of personal data referred to as Special Categories of Personal Data. The processing of this category of personal data is more sensitive because it can be more intrusive on data subjects' privacy, and that needs more protection.

This concept is not numerus clausus. Nevertheless, GDPR states that the following categories of personal data are considered sensitive data:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic and biometric data,
- Health-related data, or
- Data concerning a person's sex life or sexual orientation.

To instate the required need for additional protection, GDPR states that in order to lawfully process personal data, we need to identify:

1. A lawful basis under Article 6 GDPR, and

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. A separate condition for processing special category data under Article 9 GDPR.

There are ten conditions for the processing of the special category of personal data under Article 9 GDPR:

Article	**Condition**
9(2)(a)	Under explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
9(2)(b)	Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
9(2)(c)	Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
9(2)(d)	Processing carried out by a non-profit organisation with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
9(2)(e)	Processing relates to personal data manifestly made public by the data subject
9(2)(f)	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
9(2)(g)	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
9(2)(h)	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
9(2)(i)	Processing relates to public interest in the area of public health
9(2)(j)	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

2.3 International

The GDPR not only applies to organisations located within the European Union (EU) but also applies to organisations located outside of the EU if they offer goods or services or monitor the behaviour of EU data subjects. It applies to all companies processing and holding personal data of data subjects residing in the EU, regardless of the company's location. The GDPR also applies to the processing of personal data of data subjects inside the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens and the monitoring of behaviour taking place within the EU territory.

3. Individual rights

All data subjects can request that St. Julian's School comply with a request to exercise their rights, which are listed below.

3.1 Right to be informed (GDPR Article 13)

The right to be informed encompasses St. Julian's School's obligation to provide 'fair processing information', typically through privacy notices when personal data is being collected.

The GDPR sets out the information that should be given and when individuals should be informed.

The information given about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge.

All St. Julian's School forms where personal data is being collected should have simple and clear privacy notices, making this right to be informed.

3.2 Right of Access (GDPR Article 15)

This is the right of data subjects to obtain from St. Julian's School confirmation as to whether or not their personal data is being processed, where and for what purpose. Further, St. Julian's School shall provide a free-of-charge copy of the personal data, preferably in an electronic format.

Data subjects have the right to obtain:

- Confirmation that their data is being lawfully processed.
- Access to their personal data.
- Supplementary information if needed.

3.3 Right to rectification (GDPR Article 16)

Data subjects are entitled to have their personal data rectified if said data is inaccurate or incomplete.

If St. Julian's School discloses personal data to third parties, it must inform them of the rectification when possible. St. Julian's School must also inform the data subjects

about the third parties to whom the data will be disclosed at the time of collection.

3.4 Right to be forgotten (GDPR Article 17)

The right to be forgotten entitles the data subjects to request from St. Julian's School the erasure of their personal data and the cessation of further processing.

The right to be forgotten shall only be taken into account whenever there is no other lawful basis for the preservation and further processing of said data.

Every request to exercise this right should be previously sent to St. Julian's School Data Protection Officer (DPO) in order to prevent irreversible data loss.

3.5 Right to restrict processing (GDPR Article 18)

In some situations, this right gives the data subject an alternative to requiring data to be erased; in others, it allows the individual to require data to be held in 'limbo' whilst other issues are handled.

If the data subject requests the restriction of some processing of certain categories of personal data, St. Julian's School may only store this data until the issue is solved.

Where data is being processed automatically, the restriction should be done through technical means. This could mean moving the data to a separate system, temporarily blocking the data on a website, or otherwise making the data unavailable.

If the data have been disclosed to others, St. Julian's School must notify those recipients about the restriction on processing requests, unless doing so is impossible or involves disproportionate effort.

3.6 Right to data portability (GDPR Article 20)

The right to data portability allows data subjects to request the transfer of the personal data they have provided in order to transfer it to another organisation. This request can be made effective directly between organisations or by giving the data subject a complete file with all their personal data.

3.7 Right to object (GDPR Article 21)

The data subject shall have the right to object to the processing of his personal data on grounds relating to his particular situation.

St. Julian's School shall not process the personal data unless:

- The School demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, and/or
- for the establishment, exercise or defence of legal claims.

3.8 Right to human oversight in cases of automated individual decision-making, including profiling (GDPR Article 22)

This section addresses the use of automated decision-making, including profiling, in compliance with Article 22 of the GDPR.

Automated decision-making occurs when decisions affecting individuals are made

through algorithms or Artificial Intelligence (AI) tools without human involvement. This may include, for example, profiling students or staff for administrative or operational purposes. Article 22 foresees that any data subject has the right to request human oversight when this happens.

The School will only employ automated decision-making, including profiling, when:

- Explicit consent has been obtained from the data subject, or
- Authorised by law, provided appropriate safeguards are in place, or
- Necessary for contractual performance between the data subject and the School.

In cases where automated decisions may have significant effects on individuals, such as impacting legal rights or similarly affecting them (e.g., performance assessments or eligibility for services), the School will ensure:

- The existence of human intervention: The data subject has the right to request human intervention.
- Data subjects can express an objection: The data subject may object to the automated decision, requesting an alternative method of assessment.
- There is transparency: Information regarding the logic, significance, and consequences of such processing will be made available to the data subject.

To protect data subjects, the following safeguards will have to be applied:

- Clear information: Data subjects will be informed about the automated decision-making process, the data used, and the potential outcomes.
- Review mechanisms: Decisions resulting from automated processing will be subject to regular reviews by the Data Protection Officer (DPO) to ensure fairness, transparency, and compliance with GDPR.
- Risk assessment: Prior to implementation, any automated decision-making process will undergo a Data Protection Impact Assessment (DPIA) to evaluate privacy risks and to establish necessary safeguards.

With the implementation of these guidelines under Article 22, the School can ensure to provide data subjects the right to control over decisions that affect them significantly and support the School's commitment to ethical and responsible data processing practices.

3.9 Right To Compensation & Liability (Gdpr Article 82)

Data subjects can take legal action both against controllers and processors for compensation for pecuniary or non-pecuniary damage (e.g. damages for distress) suffered as a result of unlawful processing of their personal data. Data subjects will have a right to recover material and/or non-material damages, including loss of control over personal data or limitation of rights, discrimination, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy and "other significant economic or social disadvantage".

In the event that such rights are exercised, St. Julian's School will endeavour to ascertain clearly the identity of the requesting data subject.

4. St. Julian's School steps to ensure compliance with GDPR

4.1 Appointing a Data Protection Officer (DPO)

St. Julian's School has appointed a Data Protection Officer (DPO) to ensure its compliance with the GDPR.

The DPO shall have at least the following tasks:

- To inform and advise St. Julian's management and remaining staff who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions.
- To monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of St. Julian's School in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- To provide advice where requested as regards the Data Protection Impact Assessment (DPIA) and monitor its performance pursuant to Article 35 of the GDPR.
- To cooperate with the supervisory authority.
- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The DPO shall, in the performance of their tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

An internal document on how and when to contact the DPO is to be made available to all personnel and student community.

4.2 Raising awareness

Raising awareness on data protection matters is a big step towards GDPR compliance. St. Julian's School makes sure that decision makers and key people in the organisation are aware of GDPR.

4.3 Information St. Julian's school holds (data audit)

St. Julian's School documents what personal data is held, where it came from and with whom it is shared.

4.4 Communicate privacy information

St. Julian's School reviewed their privacy notices and updated internal procedures in order to comply with GDPR. When St. Julian's School collects personal data, there's an obligation to provide certain information, such as the controller identity and how the school intends to use their information.

4.5 Processing

Processing is defined as "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;". **This means anything you do with personal data, including deleting or archiving, constitutes processing it.**

4.6 Privacy by design, by default and data protection impact assessments (DPIAs)

The GDPR places onerous accountability obligations on organisations to demonstrate compliance. This includes requiring them to:

- Maintain certain documentation.
- Conduct a data protection impact assessment where more risky processing takes place (such as CCTV, biometric control, profiling, digital marketing, etc).
- Implement data protection by design and by default.

In this sense, St. Julian's School must ensure that privacy concerns are a key part of their decision making. GDPR seeks to ensure that the privacy rights of data subjects are prioritised by data controllers when they make internal or business decisions.

St. Julian's School will have to carry out privacy impact assessments for any actions that may pose a high risk for data subjects' privacy rights. GDPR has introduced mandatory DPIAs (Article 35). Under the Regulation, businesses will be obliged to conduct DPIAs where the processing, particularly where it utilises any new technologies, "is likely to result in a high risk" for the rights of individuals, having regard to the "nature, scope, context and purposes of the processing".

What is a DPIA?

DPIAs are prospective diligences and act as an early warning system which may affect the design/end result of a new project or practice. The final objective is to identify and reduce the privacy risks and help on the decision-making process.

Objectives

- Minimize risks
- Prevent unlawful processing
- Implement privacy by design and by default

What triggers a DPIA?

Under Article 35(1) of the GDPR, the processing of personal data likely to entail a high risk to the rights and freedoms of natural persons must be preceded by a DPIA.

The European legislator defines, by way of example, three types of situations which fulfill the conditions of this obligation of the data controller and which are laid out in Article 35(3) of the GDPR:

- Systematic and complete assessment of personal aspects relating to natural persons, based on automated processing, including profiling, and decisions which have legal effects on the natural person or which significantly affect the natural person are adopted.
- Large-scale processing of special categories of data referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
- Systematic control of large-scale publicly accessible areas.

Thus, in addition to those provided for in Article 35(3) of the GDPR, the local Portuguese data protection authority (CNPD) determined additional examples of processing of personal data that is subject to a prior DPIA, (Regulamento n1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados) as listed below:

- Processing of the data provided for in Article 9(1) or Article 10 of the GDPR for purposes or purposes other than that originally justified by its collection (in particular for the purpose of public-interest archive, scientific research or statistical purposes), with the exception of treatments provided for and regulated by law which provide adequate guarantees of the rights of the holders and is preceded by an impact assessment on data protection.
- Processing of information arising from the use of sensors or other electronic devices transmitting, by communication networks, personal data, with legal effects on the sphere of their owners or significantly affecting them in a similar way, in particular to allow analysing or predicting the location and movements, personal tastes or interests, consumption or other behavior and health (e.g., medical devices implanted or applied to people).
- Interconnection of personal data or processing relating to personal data provided for in Article 9(1) GDPR.
- Processing of personal data on the basis of indirect collection of personal data, where it is not possible or feasible to ensure the right of information pursuant to Article 14 of the GDPR.
- Processing of personal data involving or consisting of large-scale profiling.
- Processing of personal data to trace the location or behavior of their owners (e.g. workers, customers or only passers-by), except where processing is indispensable for the provision of services specifically requested by customers.
- Processing of biometric data for the unambiguous identification of its data subjects, with the exception of treatments provided for and regulated by law that have been preceded by an impact assessment on data protection.
- Processing of personal data using new technologies or new use of existing technologies.
- Significant change in the architecture of the information system on which the processing of personal data is based.

It is stressed that this list is not exhaustive and that other situations may also arise, in particular depending on technological development, in which it is justified, in accordance with Article 35(1), to carry out the DPIA. This is a dynamic list, being updated whenever it is necessary.

Those responsible for the treatment should pay due attention that the performance of such impact assessment does not exempt them from complying with the other obligations laid down in the GDPR or in special legislation.

DPIAs are particularly important in the case of:

- Systematic and extensive evaluation based on automated processing, including profiling, and on which decisions with legal or similar effects are based.
- Processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences.

- Systematic monitoring of a publicly accessible area on a large scale.
- Positive or negative lists by SAs.

What is the content of a DPIA?
St. Julian's School must assess the impact of the envisaged processing operations on the protection of personal data, of the processing and its purposes.
Including, where applicable:

- The legitimate interest pursued by the School.
- Assessment of the necessity and proportionality of the processing
- Assessment of the risks to the rights and freedoms of data subjects
- Consider expectations of the individuals
- Evaluate the level of risk, based on likelihood, and impact
- The measures envisaged to address the risks
- Including safeguards, security measures and mechanisms (for example, pseudonymisation, anonymisation, encryption, local storage, access restriction, limiting retention)
- Compliance with approved codes of conduct shall be taken into account

A suggested template for DPIAs is given below:

- Name of Project / New software / New procedure / New application.
- General name of the task process giving rise to risk.
- Specific description of the source and the exact nature of the risk.
- Potential privacy impact or damage.
- The level of risk based on the likelihood of occurrence.
- Alternative solutions and potential side effects..

4.6 International transfers

In the context of our activity, we may have to transfer personal data to third parties.

In case of student transfers such third parties may be located both within and outside the EU. Third parties who are in the EU will only have access to Personal Data where the law allows them to do so.

The School will make use of technology as an aid to transform learning activities and to provide all latest innovation in learning tools to its students, therefore the School may use some applications and software that will allow students to learn from a distance (e-learning), these applications may store personal data provided by the students, parents, staff, service providers. The School will undertake all efforts in regards to safeguarding personal data under the data protection regulation.

Where personal data is disclosed to third parties located in countries outside the EU which do not ensure an adequate level of protection for personal data, the disclosure of such personal sata will rely only on the protection of the vital interests of students, parents, staff, service providers, volunteers, candidates and interns or explicit consent as set out in Article 49(1)(f) and Article 49(1)(a) GDPR respectively, and following the recommendations of the European Data Protection Board (EDPB). The School will also adopt additional safeguard measures when such data transfers occur, such as pseudonymisation and anonymisation whenever these solutions are

possible to be applied and do not create obstacles to the learning process of the data subjects.

4.7 Data transfers to sub-processors

Where personal data processing is to be carried out by a sub-processor on behalf of St. Julian's School, only sub-processors who provide sufficient assurances regarding the implementation of appropriate technical and organisational measures, in line with GDPR requirements, will be selected. These measures must ensure the confidentiality, integrity, and lawful processing of personal data.

The engagement of sub-processors for processing personal data will be formalised through a Data Processing Agreement (DPA), which must include the following elements:

- The object and duration of the processing.
- The nature and purpose of the processing.
- The categories of personal data involved.
- The categories of data subjects concerned.
- The rights and obligations of St. Julian's School.
- The obligations of the processor include adherence to data protection standards and security protocols.
- The subcontractor's duty of confidentiality.
- The security measures are required to ensure the confidentiality, integrity, and availability of the data during processing.
- The conditions under which data should be returned or securely destroyed upon contract termination.

Furthermore, the subcontractor is prohibited from engaging other suppliers (sub-processors) for any data processing activities without the specific and prior written consent of St. Julian's School.

4.7 International data transfers to non-adequate jurisdictions

In cases where data transfers are necessary to destinations without an adequacy decision from the European Commission, additional safeguard measures must be implemented. These safeguards are intended to ensure an equivalent level of data protection in line with GDPR standards and may include:

- Standard Contractual Clauses (SCCs): Where feasible, these legally binding clauses ensure compliance with GDPR requirements in the absence of an adequacy decision.
- Binding Corporate Rules (BCRs): For multinational organisations, these rules can provide a consistent level of data protection across group entities operating in jurisdictions without adequacy.
- Additional Technical Measures: When SCCs or BCRs are used, additional technical measures such as encryption, pseudonymization, and limited data access should be applied to ensure data security during transfer.
- Specific Risk Assessment: Before initiating transfers, conduct a risk assessment evaluating the destination's legal environment to identify any risks to the data subjects' privacy rights and freedoms.

- Explicit Data Subject Consent: In limited circumstances, explicit consent from data subjects can be obtained, provided they are fully informed about the risks of the transfer due to the lack of adequate protection.

These additional measures will be applied to protect personal data and uphold data subjects' rights, ensuring all international data transfers are conducted in line with GDPR standards.

5. Processing data of subjects

Schools play a key role in the development and progress of society. They are entrusted with a teaching and guiding role for students, which demands the processing of their personal data together with those in charge of their education, such as parents, guardians or teachers. Personal data is being processed from the moment of the application, through the registration phase, the management of academic transcripts, up to the catering services, transport, etc, inherent in the normal functioning of a teaching establishment such as St. Julian's School, as well as for the start-up and development of extracurricular activities.

The GDPR identifies children as vulnerable natural persons, deserving specific protection, when processing their personal data.

St. Julian's School, in its task of making effective the fundamental right to education that constitutes its raison d'être, must also observe the fundamental right to the protection of personal data, which by not being its main activity, sometimes gives rise to doubts as to the interpretation and application of its rules.

There are key moments in order to ensure we are complying with GDPR when processing children's personal data. These moments can be addressed through questions that we should always keep in mind to avoid doubts. First of all, we should question: *Why do we need this data?* In order to identify the purpose for processing. Secondly, we should ponder if "*Is it strictly necessary for the fulfilment of our educational functions?*".

In order to comply with GDPR and answer these questions properly, we must guide the reasoning by the principles of minimisation (*collect as little personal data as possible*) and proportionality (the *loss of privacy or risk to the data subject must be clearly outweighed by the identified purpose or its result*). Only in this way will we be able to achieve the necessary consideration to advance to the next step.

If we answer the second question affirmatively, we must comply with the obligation to inform the data subject (please see the in 3.1 Right to be informed) when personal data is collected. If we respond negatively to the question, the legal basis for lawful processing should be consent.

At this stage, we will only have to decide who can legally give consent or should be informed.

Until the child turns 18 years old, the consent must be obtained and the right to be informed must be delivered to the legal guardian of the child. For new personal data collected after the child turns 18 (eighteen) years old, consent must be collected directly from the child.

Please consider section 5.2 Consent of this document for further considerations.

5.1 Lawful basis for processing personal data

For processing to be lawful under the GDPR, schools need to identify (and document) their lawful basis for the processing. There are six lawful bases listed in Article 6 GDPR:

- Consent of the data subject.
- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of a data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

In the absence of a lawful basis to process personal data, that personal data must not be processed.

Data must be collected lawfully, fairly and transparently. It must be collected for specified, explicit and legitimate purposes and mustn't be further processed in a manner that is incompatible with those purposes.

It needs to be adequate, relevant and limited to what is necessary when confronted with the purposes for which they are processed.

It must be accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, bearing in mind the processing purposes, is erased or rectified without delay.

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using inappropriate technical or organisational measures as per article 32 of the GDPR, and the SJS Management Policies and Procedures relating to IT services.

5.2 Consent

Consent must be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms and be in clear and plain language.

Consent given for the processing of personal data must be as easy to withdraw as it was to give. Consent must be “explicit” for all data, and St. Julian’s School is required to be capable of demonstrating that consent was given.

Consent requires some form of clear affirmative action. Silence or pre-ticked boxes will no longer be sufficient to constitute consent.

The GDPR allows data subjects to withdraw their consent at any time unless there’s a posterior legal basis that obliges St. Julian’s School to preserve their information.

St. Julian’s School must keep a record of how and when the consent was given for each specific purpose. In this sense, all physical forms with consent collection or online options selected by the data subject must be kept, as well as all further alterations.

More detailed information about consent for each type of data subject and data processing will be given ahead

5.3 Human resources - data of candidates applying for positions

During recruitment processes between candidates and the School, personal data is shared and gathered.

The data is collected during recruitment at the following locations:

- Delivered directly by the applicant.
- Collected on the website.
- Received by mail.
- Received through specific recruitment companies or platforms.

The data received includes, in particular, the contents of the curriculum vitae, such as name, age, date of birth, telephone, mobile phone, address, email, marital status, academic qualifications, professional experience, certificates of qualifications, and information regarding the criminal record for selected candidates.

St. Julian’s School may, in the context of compliance with its regulatory and/or legal obligations, carry out background checks gathering information about candidates with other entities.

Background checks can include general information, such as validation that the candidate did perform such functions at the previous entities we are contacting for reference, and verify, in general, the previous employer´s opinion on the professional abilities of the candidate.

Information

St. Julian's School ensures that, in the collection of personal data directly from the candidates, it provides the following information:

- The identification of St. Julian’s School as a controller and, where appropriate, its representative.
- What are the purposes of the processing for which the data is intended?
- The basis of the processing is in the case of hiring.

- The categories of personal data subject to processing.
- The mandatory or optional nature of the requested data.
- The possible consequences of not supplying the data.
- How to exercise data subject rights.
- The retention period.
- The right to submit a complaint to the National Data Protection Commission.

Personal information provided within the recruitment context may be processed for other recruitment processes other than the specific one under which it was collected, unless the candidate expressly informs St. Julian's School that they intend to limit the processing of that data only to the purposes of that specific application.

Processing purposes
Applicants' data will always be collected in accordance with applicable law and in accordance with best practices, and is intended for:

- Recruitment and selection of candidates.
- Communications relating to training initiatives or traineeships.

If St. Julian's School intends to process the data of the candidates for other purposes, it shall always provide, for each purpose, the information referred to in this chapter.

Applicants will always be assured of the possibility of exercising their rights, in particular that of being opposed to the processing of their personal data for purposes that are contrary to their wishes.

Legal basis
St. Julian's School ensures that the processing of candidates' personal data is carried out in such a way as to guarantee their lawfulness.

The fundamentals that allow St. Julian's School to perform the processing are based on:

- The need for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Consent for the processing of personal data for one or more specific purposes.
- The fulfilment of legal obligations and defence of the interests to which St. Julian's is subject, in case additional information is requested, including personal data of a criminal nature.

Data communication
In the context of the processing of candidates' data, St. Julian's School may communicate data to recruitment and selection companies, who act as subcontractors of St. Julian's School in the application process (Consent - see above).

Where necessary for the processing operations of the candidates' personal data, in particular beyond the legal obligations of the school or the fulfilment of a contract (Legal basis, first and third points - see above), obtaining prior consent from the candidates is mandatory; that consent shall be obtained through a written document, in the following terms:

- Information on the treatment that requires the applicant's consent must be presented in an accessible manner.
- The text will clearly identify the different processing purposes for which consent is being sought.
- The language used will be clear and straightforward, so that the consent provided by the applicant can be described as free, specific, informed and explicit consent.

St. Julian's School stores the date, method and content of the information provided as well as the validity, scope and willingness of the given consent.

St. Julian's School provides a simple method for the subject to withdraw their consent at any time.

5.4 Human Resources - personal data of employees

Within the contractual relationship between staff and St. Julian's School, personal data are provided and collected.

The data is collected at various times:

- During recruitment, when the potential contributor presents data that identifies it and is already identified in point 5.1. of this policy.
- At the time preceding the conclusion of the contract between the parties, at which time the contributor provides a set of data that is necessary for the conclusion thereof. This data is the information that is collected for writing up the employment contract and its execution, as well as for compliance with legal obligations with regulatory authorities, namely, tax identification number, social Security number or equivalent, IBAN account number, number of dependents, social benefits and other equivalents.
- During the execution of the contract, a set of data may be requested to manage the contractual relationship. This data is based on information that may be collected for compliance with regulatory and/or legal obligations and the internal regulations, in particular, data relating to medicine and health at work and data derived from controls on the use of Equipment and information systems.
- Employee photograph for school access card, presentation panel, Yearbook and salary processing programme.

When the data originates from other sources, St. Julian's School will provide the contributor with the information provided below, at the time of registration of the data in its databases or when the data was first made available to the third parties, and never within a period exceeding one (1) month after its collection.

Information

St. Julian's School ensures that, in the collection of personal data made directly with the staff, it provides the following information:

- The identification of St. Julian's School as a controller and, where appropriate, its representative.
- What are the purposes of the processing for which the data is intended?

- The basis for processing, namely the legitimate interest of St. Julian's School, is applicable.
- The categories of personal data subject to Processing.
- The recipients or categories of recipients of the data, in particular the legitimate interest thereof, if applicable.
- The existence of transfers of data outside the European Union and existing safeguards.
- The mandatory or optional nature of the provision of the data.
- The possible consequences of not supplying the data.
- The forms of exercising the rights of data subjects.
- The retention period.
- The right to submit a complaint to the National Data Protection Commission (supervisory Authority).

When the data is not collected directly from the staff, the information referred to above adds the indication from which source the personal data originates, and if applicable, whether it came from publicly accessible sources.

Processing purposes
Employee data will always be collected in accordance with applicable law and in accordance with best practices, and is intended for:

- Execution of the contract between the parties and the fulfilment of the obligations of St. Julian's School.
- Calculation and payment of remuneration, ancillary benefits, other allowances and gratuities.
- Payment of expenses.
- Calculation, operations relating to discounts on remuneration, mandatory or optional, arising from legal obligations.
- Attendance control.
- Performance evaluations.
- Fixing working schedules.
- Occupational medicine, safety, hygiene and health at work.
- Managing insurance.

If St. Julian’s School intends to treat the data of the employees for other purposes, the set of information referred to in this chapter shall always be provided in respect of each purpose. Employees will always be assured of the possibility of exercising their rights, particularly in opposition to the processing of their personal data for purposes that they do not agree with.

Legal basis
St. Julian’s School ensures that employee personal data is processed lawfully.

The fundamentals that allow St. Julian’s School to perform the treatments are based on:

- Consent for the processing of personal data for one or more specific purposes;
- The need for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

- Processing is necessary for compliance with a legal obligation to which St. Julian's School is subject.
- When the treatment is necessary for the pursuit of the legitimate interests of St. Julian's School.

Data communication

In the context of the processing of employees ' data, StJulian's School may communicate data to the following entities:

- IGFSS – Institute for Financial Management of Social Security,
- AT – tax authority.
- Credit institutions and financial corporations.
- INE – National Institute of Statistics.
- ACT – Authority for work conditions.
- IMT – Institute for Mobility and Transport.
- The entity that is responsible for the exercise of the functions related to safety, hygiene and medicine at work.
- Regulatory and supervisory bodies.
- Any other entity to which wage processing and/or other functions related to personnel management have been assigned.

Other entities not mentioned, but which have legal legitimacy to carry out the processing of the data in question, are not excluded.

Consent

When, in particular, beyond the need to comply with legal requirements or the fulfilment of a contract, it is necessary to obtain prior consent from the staff for the processing of their personal data, that consent shall be obtained through specific terms within the employment contract, or through a written document, in the following terms:

- Information on the Processing that requires the employee's consent should be presented in an accessible manner.
- The text will clearly identify the different processing purposes for which consent is being sought.
- The language used will be clear and straightforward.
- So that the consent provided by the collaborator is a free, specific, informed and explicit consent.

St. Julian's School stores the date, method and content of the information provided as well as the validity, scope and indication of the given consent.

St. Julian's School provides a simple method for the subject to withdraw their consent at any time.

5.5 Personal data of students

5.5.1. Data collection

In the context of the contractual relationship established between students, represented by their parents or guardians, and St. Julian's School, personal data are provided and collected for the provision of educational services.

Data are collected during enrollment at the school and throughout the School attendance period. The information is requested for the management of the contractual relationship, compliance with legal and regulatory requirements, and for communication purposes, collected through the respective forms, namely, name, sex, age, place and date of birth, nationality, telephone, mobile phone, address, email, identification documents, tax identification number, and photograph.

Information

St. Julian's School ensures that when collecting personal data directly from the parents or guardians of students, it will inform them through its collection document or on the website where the data are collected, of the following:

- The identification of St. Julian's School as a controller and, where appropriate, its representative.
- Data protection officer and their contacts.
- What are the purposes of the processing?
- The basis for processing, namely the legitimate interest of St. Julian's School, if applicable.
- The categories of personal data subject to processing.
- The addressees or categories of recipients of the data, in particular the legitimate interest thereof, if applicable.
- The existence of transfers of data outside the European Union and existing safeguards.
- The mandatory or optional nature of the provision of the data.
- The possible consequences of not supplying the data.
- The forms of exercising the rights of the data subject.
- The enrolment period.
- The right to submit a complaint to the National Data Protection Commission.

Processing purposes

Student data will always be collected in accordance with the applicable legislation and best practices, and is intended for:

- Provision of educational services.
- Management and processing of the student's eductional path.
- Class lists.
- Student Council.
- Library management.
- Organisation of travel, school transportation and excursions.
- Enrolment in extracurricular activities.
- Lost and found management.
- Management of lockers.
- School insurance and personal accident insurance.
- Sending newsletters.
- Recording and use of image and voice.

Other purposes not identified in the preceding paragraphs shall be subject to specific information and, if applicable, consent, at a time which may not coincide with registration. Examples of such situations are, in particular, processing related to psychology, prescribing of medication or health care delivery.

Students represented by parents or guardians are always guaranteed the possibility of exercising their rights, particularly in opposition to the processing of their personal data for purposes that are not appropriate to the consent provided.

Legal basis
St. Julian's School ensures that the processing of the personal data of the students is carried out to ensure their lawfulness.

The fundamentals that allow St. Julian's School to process data are based on:

- Consent for the processing of personal data for one or more specific purposes.
- The need for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Where processing is necessary for compliance with a legal obligation to which St. Julian's School is subject.
- When the Processing is necessary for the pursuit of the legitimate interests of St. Julian's School.

Data communication
In the context of data processing, St. Julian's School may communicate the student data to the following entities:

- Legal, judicial or administrative authorities, in cases where such a transfer is mandatory.
- Insurers.
- Sports centres.
- Medical clinics.
- Travel agencies.
- After-School Activities Organisers.
- Examination Boards.
- eLearning Platforms under the educational service provision.
- Others that may be necessary under the contractual relationship established with the data subject and previously communicated to them.

Consent
Where, in particular, beyond the need to comply with legal requirements or the fulfilment of a contract, it is necessary to obtain prior consent from the students/guardians, that consent shall be obtained by written document, or through the website, in the following terms:

- Information on the processing that requires the consent of parents/guardians should be presented in an accessible manner;
- The text will present the different purposes for which the data are intended individually and clearly distinguished from each other;
- The language used will be clear and straightforward in such a way that the consent provided by the student/guardians is free, specific, informed and explicit.

In the case of the use of personal data for marketing purposes, specific requests for consent will be sought.

St. Julian's School stores the date, method and content of the information provided as well as the validity, scope and indication of the given consent.

St. Julian's School provides a simple method for the data subject to be able to withdraw her/his consent at all times.

5.6 Personal data of parents/guardians

Data collection
In the context of the contractual relationship established between students, represented by their parents or guardians, and St. Julian's School, personal data from parents/guardians for contractual management is provided and collected.

Data are collected during enrollment at the school and throughout the student's school attendance period. The information that is requested for the management of the contractual relationship, compliments of legal and regulatory requirements, and for the purposes of communication and promotion of the services and products of the school, collected through the respective forms, is framed in this data Namely, name, gender, age, place and date of birth, nationality, telephone, phone, address, email, marital status, identification documents and tax identification number.

Information
St. Julian's School ensures that, in the collection of the data, it will inform through its collection document, or on the website on which the data was collected, of the following information

- The identification of St. Julian's School as a controller and, where appropriate, its representative.
- DPO and their contact details.
- What are the purposes of the processing?
- The basis for processing, namely the legitimate interest of St. Julian's School if applicable.
- The categories of personal data subject to processing.
- The addressees or categories of recipients of the data, in particular the legitimate interest thereof, if applicable.
- The existence of transfers of data outside the European Union and existing safeguards.
- The mandatory or optional nature of the provision of the data.
- The possible consequences of not supplying the data.
- The forms of exercising the rights of the data subject.
- The enrolment period.
- The right to submit a complaint to the National Data Protection Commission.

Processing purposes
Parent/guardian data will always be collected in accordance with relevant legislation and in accordance with best practices, and are intended to:

- Contractual management.
- Payment of school fees and invoicing.
- Contact details.
- Parents' Association.

- Sending newsletters and information.

Other purposes not identified in the preceding paragraphs shall be subject to specific information, and if applicable, the consent at the time may not coincide with the registration.

Parents or guardians have always ensured the possibility of exercising their rights, in particular as opposed to the processing of their personal data for purposes that are not appropriate to the consent provided.

Legal Basis
St. Julian's School ensures that the processing of the personal data of the parent/guardian is carried out to ensure its lawfulness.

The fundamentals that allow St. Julian's School to perform the Processing are based on:

- Consent for the processing of personal data for one or more specific purposes;
- The need for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Where processing is necessary for compliance with a legal obligation to which St. Julian's School is subject;
- When the Processing is necessary for the pursuit of the legitimate interests of St. Julian's School.

Data communication
In the context of data processing, St. Julian's School may communicate the parent/guardian data to the following:

- Legal, judicial or administrative authorities, in cases where such a transfer is mandatory.
- Insurers.
- Sports centres.
- Medical clinics.
- Travel agencies.
- Other entities provided that this has been previously communicated to the data subject.

Consent
Where, in particular, beyond the need to comply with legal requirements or the fulfilment of a contract, it is necessary to obtain prior consent from parents and guardians, that consent shall be obtained through a written document, or through the parents' platform, in the following terms:

- Information on the processing that requires the consent of parents/guardians should be presented in an accessible manner.
- The text will present the different purposes for which the data are intended individually and clearly distinguished from each other.
- The language used will be clear and straightforward in such a way that the consent provided by the student/guardians is free, specific, informed and explicit.

In the case of the use of personal data for marketing purposes, specific requests for consent will be sought.

St. Julian's School stores the date, method and content of the information provided as well as the validity, scope and willingness of the given consent.

St. Julian's School provides a simple method for the data subject to be able to withdraw his/her consent at all times.

5.8 Data from students and guardians, and the Internet
When the personal data of the students/guardians is collected via the Internet, the owner of the personal data is informed of the way in which their data is processed through the website privacy Policy and the cookie policy, which are available on the St. Julian's School sites. These policies are easily identifiable and contain clear and accessible language.

In the case of the use of personal data for the purpose of advertising, specific consent is sought to this effect, through an opt-in window, and is guaranteed to the data subject who may, at any time, oppose such Processing through the privacy policy that is published on the St. Julian's School website.

5.9 Personal data of former students (alumni) St. Julian's School stores personal data of former students, including name, address, email address, and profession.

Information
St. Julian's School ensures that, whenever this does not imply an unreasonable effort, it shall give the alumni the information it is obliged to provide under Article 13 of the GDPR.

Processing purposes
The alumni data is intended for:

- Contact purposes.
- Sending newsletters and information about school life,
- Historical archiving purposes.

Other purposes not identified in the preceding paragraphs shall be subject to specific information and, if applicable, consent is collected.

Alumni are always guaranteed the possibility of exercising their rights, in particular, against the processing of their personal data for purposes that are not appropriate to the consent provided.

Legal basis
St. Julian's School ensures that the processing of the personal data of the alumnis is carried out to ensure their lawfulness.

The legal basis that allows St. Julian's School to process the data is based on:

- Consent for the processing of personal data for one or more specific purposes.
- In pursuing the legitimate interests of St. Julian's School.

Data communication
In the context of the processing of data, St. Julian's School may communicate the data of alumnis to the following entities: legal, judicial or administrative authorities, in cases where such a transfer is mandatory.

Consent
Where it is necessary to obtain prior consent from the alumnis, that consent shall be obtained by a written document, or through the website, in the following terms:

- Information on the processing that requires the consent of alumni should be presented in an accessible manner;
- The text will present the different purposes for which the data are intended individually and clearly distinguished from each other;
- The language used will be clear and straightforward in such a way that the consent provided by the alumni is free, specific, informed and explicit.

St. Julian's School stores the date, method and content of the information provided as well as the validity, scope and willingness of the given consent.

St. Julian's School provides a simple method for the data subject to be able to withdraw his/her consent at all times.

5.10 What about Data Subjects under the age of 18?
Naturally, given that we are a school, this means that we process large amounts of personal data that belongs to data subjects under the age of 18. The legal basis for most of this processing is the service that we render. We are a school, and therefor,e we need to process the data of children in order to educate them.

There are, however, certain situations where we need consent in order to process data. For example, the publication of images or video requires consent as they are not essential for the provision of our educational services. i.e. we can still educate someone even if we do not publish their images. In those and similar situations, consent must be obtained from the parents or legal guardians until the child turns 18.

As regards the processing of data by online services that the school has procured and made available to the students, it is our understanding that consent is not required as the legal basis for the processing, given that these services are used as an aid to our schooling services. However, in certain cases, the use of these platforms implies the transfer of personal data outside the EU, and for that, we do need consent. In those situations, we will seek the consent of the parents or legal guardians.

But does this mean that St. Julian’s School needs to ask for new consent when the student turns 18? Not really. Regarding the data subject’s autonomy to consent to the processing of their personal data, consent by a holder of parental responsibility, or authorised by a holder of parental responsibility for the processing of personal data of children, can be confirmed, modified or withdrawn once the data subject reaches the age of digital consent. In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data, given prior to the age of digital consent, will remain a valid ground for processing.

However, after reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with article 7.3 of GDPR. In accordance with the principles of fairness and accountability, St. Julian's School must inform the child about this possibility.

6. Use of generative AI tools

6.1 Definition and scope

This chapter addresses the use of Generative Artificial Intelligence (AI) technologies, such as ChatGPT or other Large Language Model-based systems (LLM), which include tools that automatically generate content (such as text, images, and responses) through advanced machine learning models. Such technologies may support educational and administrative activities, including data analysis, educational content generation, and automated communications support. The growing use of these tools requires that St. Julian's School take steps to ensure that a safe environment exists for this solution to be used for the development of the school's teaching services and for the students' learning process.

6.2. Compliance principles

In using generative AI tools, the School is committed to adopting the following guidelines in compliance with GDPR, AI Act and other applicable laws:

- Data minimisation and anonymisation: whenever possible, anonymised or pseudonymised data will be used. Only the strictly necessary data will be processed by AI systems.
- Risk awareness: Before deploying any Generative AI tools, potential privacy risks must be assessed, particularly if such tools involve sensitive or personal data.
- Prior evaluation: The Data Protection Officer (DPO) must be consulted before implementing any generative AI tool that processes personal data, particularly in activities that could pose high risks to data subject rights and freedoms.

6.3. Transparency and data subject rights

To ensure transparency in the use of generative AI:

- Data Subject Information: Privacy notices will include information about the use of generative AI, specifying its purpose and applicable rights.
- Right to Object and Withdraw Consent: Data subjects will be ensured the right to object to decisions based on automated processing and to withdraw consent whenever AI is used to process their personal data.

6.4 Risk mitigation measures

The School shall implement the following measures to mitigate risks associated with the use of Generative AI tools:

1. Data Protection Impact Assessments (DPIAs): To ensure that generative AI use is secure and compliant with data protection regulations, a Data Protection Impact Assessment (DPIA) will be conducted in cases where:
    a. Generative AI uses personal data of students, staff, or others for profiling or behavioral analysis;

   b. There is a foreseeable high risk to privacy, such as in the analysis of sensitive data or in automated decision-making impacting data subjects.
   c. The DPIA has to include:
      i. Process Description: Detailed mapping of how AI will process and use personal data.
      ii. Risk Identification: Evaluation of potential risks to data subjects and mitigation measures.
      iii. Safeguard Measures: Action planning, including anonymisation and encryption, to ensure data security and privacy.
2. Human Oversight: Ensure human oversight over AI-generated outputs to avoid errors, bias, or misuse of data.
3. Access Control: Restrict access to Generative AI tools or LLMs and their outputs to authorized personnel only.

6.5. Training and awareness

The School must ensure that all staff involved in the use of generative AI tools are adequately trained on:

- Ethical practices: respect for privacy and data subject integrity, Ensuring a fair and transparent use of AI technologies.
- Security procedures and best practices: how to ensure that personal data is not exposed to risks through AI use, by protecting data against misuse, breaches, or unauthorized access
- Anomaly detection and reporting: the capacity to identify and quickly report anomalies or potential data breaches to the data protection team.

6.6 Specific use cases and limitations

St. Julian's School commits to using Generative AI or LLM tools only for legitimate and well-defined purposes, such as:

- Administrative efficiency: automating repetitive tasks while ensuring data security.
- Educational enhancement: supporting personalised learning or content creation while respecting privacy.
- Operational support: assisting in communication or resource allocation without impacting data subject rights.

Generative AI tools must not:

- Be used to make legally binding or significant decisions without human intervention.
- Process sensitive or personal data without robust safeguards and explicit legal justification.

6.7 Special Considerations for LLMs

- Data retention: LLMs often do not "store" specific input data permanently, but users should ensure that sensitive input is not cached or logged by the system provider.
- Model bias: LLMs are trained on large datasets and may reflect biases present in that data. Regular reviews and fine-tuning are necessary to align outputs with ethical and legal standards.

- Provider compliance: when using third-party LLMs, ensure that the provider complies with GDPR and any applicable data protection laws, especially for international data transfers.

6.8 Special consideration for minors when using AI tools

In line with Article 5 of the AI Act and the School's Data Protection Policy (see sections 5.5 and 5.8), the School recognises that students under the age of 18 are particularly vulnerable to the potential risks posed by AI systems. Where Generative AI tools are used in contexts that may involve student data, the School will apply enhanced safeguards and ensure that no AI-generated outputs result in profiling, manipulation, or automated decision-making that could negatively affect students' rights, development, or well-being.

7. Data breaches

A data breach occurs when the security or integrity of personal data is compromised. This can occur through misappropriation; loss or theft of data or equipment; unauthorised individuals gaining access; a deliberate attack on systems; equipment failure; human error of malicious acts such as hacking, viruses or deception.

Under the GDPR, data breach notification becomes mandatory where it is likely to "result in a risk for the rights and freedoms of individuals".

St. Julian's School needs to document any facts relating to a data breach event.

In this context, St. Julian's School created a Guide on Data Breach Management and Procedures to be followed when such situations arise.

If any member of St. Julian's School community has information relating to a possible data breach situation should immediately contact the Data Protection Officer.

Without prejudice to the provisions of the security rules of the media and information of the St. Julian's School, in the event of a personal data breach, the National Data Protection Commission shall be notified within 72 hours.

The occurrence shall likewise be communicated to the data subjects without undue delay if they are concerned with sensitive data.

The notification to the National Data Protection Commission shall include:

- Description of the nature of personal data breach, including the categories and number of data subjects affected, as well as the categories and number of data records concerned.
- Information on the identity and contacts of the data protection officer or other contact point where additional information can be obtained.
- Description of the consequences of a personal data breach.
- Description of the measures proposed or adopted to resolve the breach of personal data, and, if possible, reduce its effects.

The communication to the data subjects shall contain the information provided for in points second, third ancd fourth points above.

Personal data breaches are documented, including the facts relating thereto, their effects and the remedial measures taken.

8. Roles and responsibilities

Everyone within St. Julian's School has a role to play in ensuring that the School can evidence compliance with data protection laws. The main parties responsible for the enforcement of this policy are the Head and the Bursar (Director of Operations and Finance), supported by the schools DPO in an advisory role and the existing GDPR Governance Team (Whole-School Leadership).

St. Julian's School took the opportunity and reviewed staff practices and personal data forms and the way they were collected. Everyone at St. Julian's School should consider and ask for training on privacy matters, especially on roles or departments with regular contact with personal data collection activities.

All members of the St. Julian's School community shall only use the latest and approved version of templates and forms in which personal data is collected.

St. Julian's School staff shall consider all the internal policies and procedures in order to ensure a high level and appropriate compliance regarding privacy and personal data protection.

Below you can find the ways each person within the School community can help.

The Head and Burasr

- Appointing and supporting Data Protection Officer..
- Discuss data privacy related issues in their meetings.

GDPR Governance Team (WLT)

- Review the implementation, effectiveness, and compliance with policies, procedures, protocols.
- Key role in driving data protection awareness and compliance..
- Developing policies, procedures, and protocols.
- Promoting privacy and data protection awareness sessions..
- Identifying training needs..
- Taking preventative actions to mitigate the risk of data breaches arising.
- Coordinate with DPO and IT the data breach protocol and procedures..
- Due diligence of service providers (data processors) prior to any decision..
- Ensuring appropriate written contracts with all service providers (DPAs.).
- Consider the DPIA's' results in the decision-making..
- Overseeing data subject right requests..
- Working closely with the DPO and IT..

Teaching Staff / Schoolkeepers / Security

- Security of school buildings: locking gates, locking doors, locking cabinets.
- Ensure alarms are switched on (and working).
- Ensure that CCTV systems are working and are maintained appropriately.
- Ensure that only authorised persons have access to school buildings.
- Storage of confidential wastepaper until it is securely shredded..
- Report any personal data breaches immediately to the DPO and Bursar.
- Comply with and give assistance during audits, due diligences and inspections..
- Ensure professional documents are stored under advanced security safeguards..
- Ensure confidentiality about health-related information regarding students..
- Comply with email usage policy..
- Be aware of the risks regarding social networks publications..
- Respect access-permission levels..

Administrative Support Staff / Receptionist / School Secretaries

- Keep the reception area clean and tidy..
- Ensure that personal data is not visible to others (eg, leaving files on the desk).
- Keep personal data documents out of sight..
- Ensure computer screens are not visible to visitors or strangers..
- Diligence and attention to detail when entering personal data into school systems..
- Keep the data accurate, complete, and up-to-date.
- Identify data subject requests when they are received (by letter, email, etc)..
- If a request is received by telephone, ask the person to put their request in writing..
- Ensure that all requests shall be immediately communicated to the DPO..
- Be cautious about requests for information: when a request for personal data is received, ask the requester for information to verify their identity, ascertaining whether the requester is legally entitled to obtain the personal data..
- Be suspicious: alert to the possibility of impersonation, trickery, deception, phishing, social engineering, etc.
- Prepare posts with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope. Developing post protocol checklist (eg, double-checking enclosures, envelope counts, etc).
- Prepare emails with high levels of diligence and attention to detail:
    - Ensure that the correct email address is entered.
    - Use “bcc” instead of “to” or “cc” field where appropriate.
    - Encrypt emails where appropriate.
        - If the email is sent to a group, verify the group members.
    - Be cautious and suspicious if an email asks you to click on links or open an attached document (even if from a familiar sender with a genuine email address).
- Immediately report to IT any suspicious email received.
- Respect access-permission levels..

IT Team

- Keep anti-virus and anti-malware software up to date, and install patches when required.
- Ensure that data is kept safe and secure..
- Use strong passwords (12 characters, a mixture of alphanumeric, upper and lower-case, and symbols) and change them regularly..
- Never share login credentials. Never allow someone else to see you entering passwords (particularly students)..
- Immediately notify the Bursar and/or DPO if anyone attempts to obtain unauthorised access to personal data..
- Ensurea quick response to reported suspicious activity..
- Grant access to school platforms and systems to each user according to the defined criterion..
- Handle regular audits of the school system security..
- Supervise users' compliance with equipment usage policies..
- Work closely with DPO and the Busrar..

School Nurses / Doctor

- Adhere to ethical standards required by their professional bodies regarding confidentiality and record keeping..
- Have a clear understanding of when and in what circumstances data should be shared (for example, child protection, child welfare, medical needs)..
- Take responsibility for keeping sensitive datasets safe and secure..
- Ensure compliance with the specific guidelines regarding the processing of health-related data.
- Ensure consent is given when applicable..
- Ensure additional security measures on files kept on personal devices or agendas.

9. Special concerns on photographs/videos, apps and social media publications

Use of apps in the educational environment

Devices and apps touch nearly every aspect of the data held by St. Julian's School.

Important procedures to bear in mind:

- Protect the LAN with antivirus, firewall, and physical protection.
- Educate students and staff on best practices for home computers.
- Create clear terms and conditions.

Use of cloud storage systems in the educational environment

Important procedures to bear in mind:

- Audit data that websites collect automatically (cookies).
- List first and third-party cookies.
- Check online forms for end-to-end security.
- Check consent processes for GDPR compliance.
- Create a privacy declaration documenting.

    - What information is being collected?
    - Who is collecting it?
    - How it is being collected?
    - Why is it being collected?
    - How it will be used?
    - Who will it be shared with?
    - If the intended use is likely to cause individuals to object or complain?
- Use strong passwords (12 characters, a mixture of alphanumeric, upper- and lower-case, and symbols) and change them regularly.
- Patch web vulnerabilities.

Photographs and videos taken inside the school premises
Children enjoy specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned as well as their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing.

If images are taken from the school with an educational purpose (e.g. work carried out for the school), the school is not authorised for the processing them without specific consent.

Images or audio recordings captured for strictly pedagogical purposes do not require consent as a basis for processing and rather fall into the scope of the school's legitimate interest. Nevertheless, such captures are not to be made publicly available. If they are used for purposes other than pedagogy, then explicit consent must be obtained.

If taking images does not correspond to the educational activity of the school (e.g. images of events that are taken mostly with the purpose of publishing them on the school magazine or on the school website), consent of the data subjects will be mandatory, and school will inform previously about the purpose of the pictures and, especially, about the existence of the possibility that the picture will be accessible indiscriminately or, on the contrary, will be limited to the school community.

When possible, it is recommended to publish this content in a private area of St. Julian's School website or platforms where it is necessary to access through identification and password.

School is not obliged to get consent for every photo and is not obliged to renew that consent every time.

Rules for using photos and videos

Photos, Videos or Audio Recordings of School Events and everyday life that are not for pedagogical purposes

Students
St. Julian's School is aware that, for most situation,s consent is required before photos or videos are published.

For some publication platforms, such as the Alumni, Parents and Summer School Portals, a dedicated consent request mechanism has been set in place, which allows users to inform the school of their wishes as regards publications of images or videos on these platforms.

For all other publication media, the sSchool has defined two broad categories of image medium publication: external or internal. The different channels the school may use, and their category, are identified in the Student Image Consent Form and on the Publication Medium Table present in the St. Julian's Image Capture Procedure document. In order to assess the consent status of students as regards these two broad categories, the school issues a yearly request for consent sent to parents or guardians. This consent may be withdrawn or changed at any time and any changes will only apply to future publications.

At times and for specific events, parents may wish to alter the consent status of students. For this purpose, the school provides an ad-hoc consent status form which establishes the consent status of particular students as regards a specific event and medium(s) of publication.

In the case of group photos or videos, the School may engage in selective blurring so as to make identification of specific students impossible if they have not expressed consent for that specific publication.

School events may be broadcast live. This live stream will be active for a limited period of time, and access will be granted by password. Consent will be requested through the annual image consent form.

Staff
Staff members are also invited to express their consent status as regards publication of photos, videos or audio recordings and the school provides means for this to be expressed.

The one exception to this is the official class photographs, where the legal basis for their processing (publication) can be found in the need for the performance of a contract to which the data subject is party in accordance with Article 6, 1 (b) of the GDPR. This information is provided to staff in accordance with Article 13 of the GDPR.

Data subjects external to the School
Sometimes it may happen that persons, not belonging to the school, may appear in captures that the School may wish to publish. In such cases, the School will endeavour to obtain the required consent before publication. If such consent is not obtainable, then blurring of such persons may occur.
Photos, videos or audio recordings for pedagogical purposes

The School understands that sometimes images, videos or audio recordings may be captured for pedagogical purposes. In such cases, the basis for processing is the school's legitimate interest as an educational establishment in accordance with Article 6 1(f) of the GDPR. In such situation,s explicit consent might not be sought.

Nevertheless, these will typically only be used internally. If at any point there is an intention to use these outside the internal school community, then an explicit consent, for that purpose, will be sought.

Communication on school events on the website and social networks: general guidelines

School events will be reported on the website and social networks. In these publications, only group photos should be used whenever possible. In social networks, only group photos will be used, and generic images should be opted for when this is not possible (logos, buildings, landscapes, etc). In cases where the groups participating in the activity are small, thereby making persons more easily identifiable, the consent expressed when signing the school's image consent form is considered valid and sufficient.

In the case of school events involving the participation of reduced groups of students, who have been selected to participate in these events, or in the case of school or Inter-school events in which specific students have distinguished themselves, and in which it makes sense to refer to the name of specific students, specific consent must exist / will be requested from their guardians for the publication of the name and/or photograph on the website and/or social networks of the school (it being possible to authorize one and not the other, or vice versa) . In cases where this has recognised relevance, the school year that the student attends may be published, but never their specific form.

Generic school publications

In the case of brochures and other promotional materials, the use of very explicit plans of the students should be avoided. Specific authorisations will be requested from minors and older pupils whose photographs are identifiable.

In the case of promotional videos, the use of very explicit close-ups of the students should be avoided. If this proves to be indispensable, specific consents will be requested from the parents or guardians of students who are identifiable in the video.

In the case of the use of photographs of students on generic pages of the website not related to school events in which they have participated (e.g. "admissions section of the website"), the use of very explicit plans of the students should be avoided. If this proves to be indispensable, specific consents will be requested.

Photos and videos captured by staff, guardians and external persons

Photographs taken by the staff of the school in private or with recourse to their own means

In general, it is advised not to capture private photographs of school students. In cases where this is necessary or relevant, for example, due to the unavailability of the multimedia team at a school event (pedagogical activity, class trip, tour), the photographs must be transmitted to the colleagues responsible for their publication (Marketing, multimedia). Personal storage is permitted, but it is expressly prohibited to share with third parties (including parents and guardians) or on digital platforms or social networks.

Share photos with students or parents/guardians
Staff can share photos with parents/guardians showing students either isolated with their parents/guardians or on their own. They may not, by any means, share with parents/guardians, photographs in which other children are identifiable, without the express permission of their parents/guardians (e.g. via WhatsApp and other means).

Photographs taken by external persons
Unless prior consent has been given, it is prohibited for persons outside the school community to photograph or film students and staff.

Photographs taken by parents/guardians to other students
Parents/Guardians are not allowed to photograph or film students other than their own, without prior consent from their parents/guardians.

Regarding image capturing and publishing, the school has defined specific guidelines to be complied with. These guidelines are to be made available to all participating parties.

Use of social networks and the website of St. Julian's School

Enforce secure communications through HTTPS
If the application does not require any form of authentication, then HTTPS might not seem needed. But it is easy to overlook some things. For instance, some applications collect personal information through their "contact us" forms. If this information is sent in clear text, it will be exposed on the Internet. Also, the IT department will make sure that the SSL certificate has been properly deployed and is not exposed to vulnerabilities related to SSL protocols.

Inform users about and encrypt personal data from 'contact us' forms.
Applications collect information not only through authentication or subscription, but also through contact forms. Most of this information is personal, including email address, phone number, and country of residence. Users must be informed how this data will be stored and for how long. The use of strong encryption is highly recommended for storing this information.

Make sure sessions and cookies expire and are destroyed after the user logs out.

Users must have proper visibility of the use of cookies by the application. They must be informed that the application is using cookies. The application should provide the opportunity for users to accept or deny cookies. Cookies must be properly destroyed after inactivity or logout.
Inform users about any data sharing with third parties

Photographs used for marketing purposes
Specific informed consent for these images and only use them online with the consent provided. Please note that St. Julian's School has updated all the forms in order to collect consent from data subjects that specifies their authorisation for online publication of their videos and/or photographs. The person in charge of publishing

these contents must ensure that all can be published according to the data subjects' preferences.

10. Final considerations / provisions

Enforcement of policy and non-compliance
Updates to the policy contained in this document shall be valid from the date of their approval. All employees of the St. Julian's School are obliged to know the content of this policy and its subsequent updates.

Collaborators are obliged to comply with this policy and to collaborate in its application. Failure to comply with these rules may lead to disciplinary action. The lack of knowledge of this policy does not justify any kind of non-compliance.

Employees should refrain from any behaviour on which they have doubts and may request the designated DPO team by sending an email to dpo@Stjulians.com for any clarifications.

In the event of a conflict between the data protection and privacy policy and the legislation, the legislation prevails over the privacy and data protection policy.

Review and monitoring of the Data Protection Policy.
This policy shall be revised periodically or where, by virtue of the needs arising from the activity of the St. Julian's School, facts, or legislative changes, so demands it.

Communication and Disclosure.
After approval, this policy will be disclosed to the staff of the school and published on the school's intranet.

Related policies
Online Safety Policy

AMENDMENTS	
New policy published.	June 2022
Minor revisions, including a new chapter on the use of AI generative tools.	May 2025

POLICY APPROVAL	
Reviewed	April 2025
Approved by the Policies & Compliance Subcommittee	8 May 2025
Approved by the Board of Governors	23 June 2025
Next review	April 2026