MISY | Mandalay
Myanmar International School Yangon (Mandalay Campus)

Myanmar International School of Yangon (Mandalay Campus)

Data Protection Policy

Approved by:	Ei Ei Zin (BOD)	**Date:** July 23, 2023
Last reviewed on:	July 2024	
Next review due by:	July 2025	

Glossary of terms:

Data protection: The process of safeguarding important information from corruption, compromise or loss.
Personal data: Any information which relates to an identified or identifiable natural person. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data
Data subjects: All people who we hold personal data for (parents, students etc)
Data controller: Myanmar International School of Yangon (Mandalay)
Data processor: The person/people responsible for processing the data
Data stewards: Designated staff members who are responsible for determining the purposes for which, and the manner in which, personal data is processed within different areas of the school.
Privacy notice: Written communication with the data subjects to let them know how and for what purpose their personal data is being processed.

Introduction

Myanmar International School Yangon (MISY) is guided by the laws and regulations relating to data protection in the Republic of the Union of Myanmar. Additionally, MISY is guided by internal policies and procedures which enable MISY to meet all relevant domestic and international obligations

MISY supports the data protection rights of all those with whom it works, including, but not limited to, staff, students, parents, visitors and alumni. This policy sets out the accountability and responsibilities of the school, its staff and its students to comply as much as possible with the provisions of the policy. MISY holds and processes personal data about individuals such as employees, students, graduates and others, defined as ‘data subjects’.

Purpose of the policy

The policy sets out the responsibilities of the school, the board of directors, the parents, the staff and the students to comply as much as possible with any laws relating to data protection within the Republic of the Union of Myanmar and internal policies and procedures which enable MISY to meet all relevant domestic and international obligations It is accompanied by a data protection handbook which provides information and guidance on different aspects of data protection for specific departments. This policy and the handbook form the framework which everybody processing personal data should follow to ensure compliance with data protection policy.

Scope of the policy

This policy applies to the board of directors, parents, staff and students in all cases where MISY(Mandalay) is the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

Status of the policy

Compliance with this policy is a condition of employment for all staff and it is an expectation that all board members, parents and students abide by the school’s policies and procedures. Contractors and external organisations working with the school will be asked to comply with these standards.

Responsibilities under the policy

MISY as a data controller has a responsibility to implement and comply with our data protection policy. This responsibility is delegated to data stewards in each area.

Data security

All users of personal data within the school must ensure that personal data is always held securely and is not disclosed to any unauthorised third party either accidentally, negligently or intentionally.

Privacy notices

When the school collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that the school must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data is processed. Any data processing must be consistent or compatible with that purpose.

Conditions of processing

In order to meet the requirements of this policy, processing personal data must meet at least one of the following conditions:

1. The data subject has given consent.
2. The processing is required due to a contract.
3. It is necessary due to a legal obligation.
4. It is necessary to protect someone's vital interests (i.e. life or death situation).
5. It 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.
6. It is necessary for the legitimate interests of the controller or a third party.

For special categories of personal data, at least one of the following conditions must be met:

1. The data subject has given explicit consent.
2. The processing is necessary for the purposes of employment and local government requirements.
3. The processing is necessary to protect someone's vital interests.
4. The processing is carried out by a not-for-profit body.
5. The processing is manifestly made public by the data subject.
6. The processing is necessary for legal claims.
7. The processing is necessary for reasons of substantial public interest.
8. The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
9. The processing is necessary for public health.
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards which are explained in the Handbook.

Data retention

Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted.

Data retention guidelines are as follows:

- Past employees: 10 years
- Past students: minimum 10 years. Maximum 15 years
- Applications not completed for potential employees and students: 3 years

Data protection by design and default

MISY has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

Data protection impact assessment

When considering new processing activities or setting up new procedures or systems that involve personal data privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an afterthought.

Anonymisation and pseudonymisation

Further mechanisms of reducing risks associated with handling personal data are to apply anonymisation or pseudonymisation. Wherever necessary, personal data must be anonymised or, where that is not possible pseudonymised.

Responsibilities of management and data users

The board of directors (BOD) will approve this policy at each review, ensure it complies with the law and hold the head of school to account for its implementation.

The board of directors will appoint a person from the BoD to monitor the effectiveness of this policy.

The BOD will have access to other related documents as approved by the head of school which apply to this data protection policy.

The BOD will have final authority in handling the data in case of emergency, breach of authority, legal situation represented as ETS Co., Ltd.

The head of school and all staff with the responsibility for the management of data has a responsibility to ensure compliance with this policy, and to develop and encourage good information handling practices within their areas of responsibility. All users of personal data within the school have a responsibility to ensure that they process the data in accordance with the principles and the other conditions set down in this policy. The data protection handbook provides detailed guidance to assist with fulfilling these obligations.

Handling research data

Before commencing any research, which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy and the guidance contained in the data protection handbook and how these will be properly complied with. The researcher must ensure that fairness and transparency is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised at the earliest possible time.

Handling of personal data by students

The use of personal data by students is governed by the following:

- Where a student collects and processes personal data in order to pursue study with the school, and this course of study is not part of a school-led project, the student rather than the school is the data controller for the personal data used in the research. If the data are extracted from a database already held by the school, the school remains the data controller for the database, but the student will be the data controller for the extracted data.
- Once a piece of work containing personal data is submitted for assessment, the school becomes the data controller for that personal data.
- Where a research student processes personal data whilst working on a project led by a member of staff, the school is the data controller.

All staff must ensure that students they supervise are aware of the following:

- A student should only use personal data for a school-related purpose with the knowledge and express consent of an appropriate member of staff.

- The use of school-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

Data subject rights

Subject access requests and the right to data portability

Individuals have the right to request to see or receive copies of any information the school holds about them, and in certain circumstances to have that data provided in a structured, commonly used and electronic format so it can be forwarded to another data controller. The school must respond to these requests within four weeks. Erasure of requested personal data must be restricted before fulfilling the subject access request.

Right to erasure, to restrict processing, to rectification and to object

In certain circumstances data subjects have the right to have their data erased. This only applies:

- Where the data is no longer required for the purpose for which it was originally collected.
- Where the data subject withdraws consent.
- Where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require the school to rectify inaccuracies. In some circumstances, if personal data is incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Individuals receiving any of these requests should not act to respond but instead should contact the head of school.

Rights in relation to automated decision making and profiling

In the case of an automated decision making and profiling that may have significant effects on data subjects, they have the right to either have the decision reviewed by a human being or not be subject to this type of decision making at all. Their requests must be forwarded to the head of school immediately.

Data sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice needs to be provided to the data subjects.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the school and the third party must be signed, unless disclosure is required by law, such as certain requests from government department offices where the third party requires the data for law enforcement purposes.

Personal data can only be transferred out of the Republic of the Union of Myanmar when there are safeguards in place to ensure an adequate level of protection for the data. Staff involved in transferring personal data to other countries must ensure that an appropriate safeguard is in place before agreeing to any such transfer and must comply with related Myanmar laws.

Direct marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For MISY, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging. The school must ensure that it always complies with school policy and, where applicable, national legislation, every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

Data protection training

Data protection training will be provided annually and will be part of the induction process for all staff.

Data protection breaches

MISY is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The school makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of the School's Data Protection Officer who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the case must be brought into the attention of the Head of School as soon as possible, and not later than 48 hours after becoming aware of it.

Related policies:

Safeguarding Policy and procedures
Admissions policy

Related Forms:

Data privacy notice