PIMSAT
INSTITUTE OF HIGHER EDUCATION

Privacy and Data Protection Policy

PIMSAT Karachi

Effective Date: 15-5-2010

Introduction:

At PIMSAT, we recognize the importance of protecting personal data and maintaining the privacy and confidentiality of our students, staff, and other stakeholders. This Data Protection Policy outlines our commitment to complying with applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR) and any relevant local data protection laws.

Scope:

This policy applies to all personal data collected, processed, stored, or shared by PIMSAT in the course of its activities. It applies to all employees, contractors, students, and any third parties who handle personal data on behalf of the institute.

Definitions:

Personal Data: Any information relating to an identified or identifiable individual.

Data Protection Office: A dedicated person, ensuring the privacy, security, and confidentiality of personal data and upholding the rights of individuals in accordance with applicable data protection laws.

Data Controller: The entity that determines the purposes and means of processing personal data.

Data Processor: A person or entity that processes personal data on behalf of the data controller.

Data Collection and Processing:

4.1. Lawfulness and Transparency:

Personal data will only be collected and processed in a lawful and transparent manner.

Individuals will be informed about the purposes and legal basis for collecting their data.

4.2. Purpose Limitation:

Personal data will be collected for specific, explicit, and legitimate purposes.

Data will not be further processed in a way incompatible with these purposes.

4.3. Data Minimization:

Only necessary and relevant personal data will be collected.

Data will be limited to what is necessary for the specified purposes.

4.4. Accuracy:

Reasonable steps will be taken to ensure the accuracy of personal data.

Data will be kept up to date, and inaccurate or incomplete data will be rectified or erased.

4.5. Storage Limitation:

Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected, unless legal requirements dictate otherwise.

Data will be securely disposed of when no longer needed.

4.6. Security Measures:

Appropriate technical and organizational measures will be implemented to protect personal data from unauthorized access, loss, destruction, alteration, or disclosure.

Regular security assessments will be conducted to identify and address potential vulnerabilities.

4.7. Data Subject Rights:

Individuals have the right to access, rectify, erase, restrict processing, and object to the processing of their personal data.

Requests related to data subject rights will be promptly addressed and responded to in accordance with applicable laws.

Data Sharing and Transfer:

5.1. Third-Party Processors:

Personal data may be shared with third-party processors who provide services to PIMSAT.

All third-party processors will be carefully selected and required to implement appropriate data protection measures.

5.2. International Data Transfers:

If personal data is transferred to countries outside the European Economic Area (EEA) or any other jurisdiction with data protection laws, appropriate safeguards, such as standard contractual clauses or adequacy decisions, will be implemented.

Policy statement

When acting as a Data Controller PIMSAT has a responsibility to implement and comply with applicable privacy and data protection laws and regulations. When Processing Personal Data, the Institute must abide by seven principles of data protection:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;
- integrity and confidentiality; and
- accountability.

Data security

All New School users of Personal Data must ensure that such data is always held securely and not disclosed accidentally, negligently, or intentionally to any unauthorized third party. The Information Security Policy, the Acceptable Use Policy, and the Standard for Handling Institutional Information must be read in conjunction with this Privacy and Data Protection Policy.

More information can be found in the Data security section of the Handbook.

Privacy notices

When PIMSAT collects Personal Data from individuals, the requirement for "fairness and transparency" must be adhered to. More information can be found in the Privacy notices section of the Handbook.

Conditions of processing / lawfulness

In order to meet the "lawfulness" requirement, the Processing of Personal Data must meet at least one the following conditions:

- the Data Subject has given consent to the Processing of their Personal Data for one or more specific purposes;
- the Processing is necessary for the performance of a contract to which the Data Subject is party;
- the Processing is necessary for compliance with a legal obligation to which PIMSAT is subject;
- the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in PIMSAT; or

- the Processing is necessary for the purposes of the legitimate interests pursued by PIMSAT or by a third party.

For Special Categories of Personal Data, at least one of the following conditions must also be met:

the Data Subject has given explicit consent to the Processing of their Special Categories of Personal Data for one or more specific purposes;

- the Processing is necessary for the purposes of employment, social security, and social protection law;
- the Processing is necessary to protect someone's vital interests;
- the Processing is carried out by a not-for-profit body;
- the Processing is manifestly made public by the Data Subject;
- the Processing is necessary for legal claims;
- the Processing is necessary for reasons of substantial public interest;
- 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;
- the Processing is necessary for public health; or
- the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to certain safeguards.

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 desktops, laptops or mobile devices, or held on paper. If the data is no longer required, it must be securely deleted or destroyed.

Privacy by design and by default

PIMSAT has an obligation to consider the impact Processing activities may have on data privacy. This includes implementing appropriate technical and organizational safeguards to minimize the potential negative impact Processing can have on the Data Subjects' privacy, both at the time of the determination of the means for Processing and at the time of the Processing itself.

Data Protection Impact Assessment

When contemplating 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 performed. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimize or reduce risks during the design stages of a process and throughout the life cycle of the initiative. This will ensure that privacy and data protection control requirements are not an afterthought.

Anonymization and pseudonymization

To further reduce the risks associated with handling Personal Data, Anonymization or Pseudonymization should be applied to the data. Wherever possible, Personal Data must be Anonymized or, where that is not possible, Pseudonymized.

Data subject rights

PIMSAT, when acting as a Data Controller, endeavors to provide Data Subjects with privacy rights that include:

- the right of access;
- the right to rectification;
- the right to erasure ("right to be forgotten");
- the right to Restriction of Processing;
- the right to be informed;
- the right to data portability;
- the right to object; and
- the right not to be subject to a decision based solely on automated Processing, including Profiling.

Data subject access requests and the right to data portability

Individuals have the right to request to see or receive copies of any Personal Data institute holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine-readable format so it can be forwarded to another Data Controller.

Workforce Members receiving a data subject access request must follow the data subject access request procedures contained in the Data subject rights section of the Handbook.

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

In certain circumstances Data Subjects have the right to have their Personal Data erased. This only applies

- where the data is no longer required for the purpose for which it was originally collected, or
- where the Data Subject withdraws consent, or
- where the data is being Processed unlawfully.

In some circumstances, Data Subjects may not wish to have their Personal Data erased but rather have any further Processing of the data restricted.

If Personal Data is inaccurate, Data Subjects have the right to require PIMSAT to rectify inaccuracies. In some circumstances, if Personal Data is incomplete, the Data Subject can also require the Institute 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 must 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.

Workforce Members receiving any of these requests should not act or respond but instead should contact the Information Security and Privacy Office immediately.

Rights in relation to automated decision making and profiling

In the case of 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 to not be subject to this type of decision making at all. These requests must be forwarded to the Information Security and Privacy Office immediately.

Data sharing

When Personal Data is transferred internally from one New School organizational unit to another, the receiving unit must only Process the data in a manner consistent with the original purpose for which it was collected. If Personal Data is shared internally for a new and different purpose, a new privacy notice must 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 Institute and the third party must be signed, unless disclosure is required by law or the third party requires the data for law enforcement purposes.

More information can be found in the Data sharing section of the Handbook.

Transfers of personal data outside the PIMSAT

Personal Data may only be transferred out of the European Economic Area when there are safeguards in place to ensure an adequate level of protection for the data. For transfers of Personal Data to a receiving party in the United States, the Privacy Shield Agreement between the European Union and the United States of America provides sufficient protection. Before transferring data, the Privacy Shield website should be consulted to determine whether the receiving party is on the Privacy Shield List.

If the receiving party is not on the Privacy Shield list, then the contract between the receiving party and PIMSAT must include a Data Processing Addendum that incorporates the European Commission's Standard Contractual Clauses for data transfers between EU and non-EU countries (either the controller-to-controller or controller-to-processor clauses, as appropriate).

Workforce Members involved in transferring Personal Data to other countries must ensure that appropriate safeguards are in place before agreeing to any such transfer.

Direct marketing

Direct marketing covers not only the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For PIMSAT, this includes notifications about

events, fund raising, and offering of goods or services regardless of whether a payment by the Data Subject is required. Marketing covers all forms of communications, such as contact by post, fax, telephone, and electronic messages. The Institute must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

More information can be found in the Direct marketing section of the Handbook.

Websites

All websites and web applications operated by or on behalf of PIMSAT must include:

A prominent link, on every page, to a privacy notice that describes how the website collects Personal Data and how that data is used, stored, transferred, and protected.

A prominent message, displayed when a user first visits the site and every time thereafter until the user affirmatively acknowledges it, seeking the user's consent to store "cookies" on the user's computer.

More information can be found in the Websites section of the Handbook.

Training

Any individual within the scope of this policy must complete the Privacy and Data Protection Training.

Breaches

PIMSAT is responsible for ensuring appropriate and proportionate security for the Personal Data that it holds. This includes protecting the data against unauthorized or unlawful Processing and against accidental loss, destruction, or damage. The Institute makes reasonable efforts to avoid privacy and data protection incidents, however, it is possible that incidents will occur on occasion. For example, Personal Data Breaches might occur through:

Unauthorized or accidental disclosure, modification, or deletion

Theft or loss of data or equipment

Unauthorized access

Hacking attack

Human error

If a Personal Data Breach occurs, the Institute may be required to notify relevant authorities in a timely manner. Any member of the Institute community who encounters something they believe may be a Personal Data Breach must report it immediately to IT Central and the Information Security and Privacy Office.

Details of how to report a breach and the information that will be required are included in the Personal Data breaches section of the Handbook.

Roles and responsibilities

The Information Security and Privacy Office and the Privacy and Security Compliance function within the Information Technology department monitor and advise on compliance with applicable privacy and data protection laws and regulations. However, responsibility for compliance and the consequences of any breaches remains with the President's Leadership Team and the Data Owners in individual organizational units. Information and advice can be obtained from the Information Security and Privacy Office and the Office of the General Counsel.

Data Owners

Data Owners are responsible for maintaining the protection of datasets containing Personal Data by ensuring compliance with this policy and applicable privacy and data protection laws and regulations, and by developing and encouraging good information handling practices among their datasets' communities of users.

Data users

All users of Personal Data within the Institute have a responsibility to ensure that they Process the data in accordance with the principles of data protection and the other conditions set forth in applicable privacy and data protection laws and regulations.

Handling research data

Before beginning any research that will involve obtaining or using Personal Data and Special Categories of Personal Data, researchers must give proper consideration to this policy and the guidance contained in the Handbook and how these will be properly complied with. Researchers must ensure that the fairness, transparency, and lawfulness principle is adhered to and that privacy is applied. This means, among other things, that wherever feasible, research data must be Anonymized or Pseudonymized at the earliest possible time.

The use of Personal Data by students is governed by the following:

Where a student collects and Processes Personal Data in order to pursue a course of study with the Institute, and this course of study is not part of a Institute-led project, the student rather than the Institute is the Data Controller for the Personal Data used in the research. If the data are extracted from a database already held by the Institute, the Institute remains the Data Controller for the database, but the student will be the Data Controller for the extracted data.

Once a thesis containing Personal Data is submitted for assessment, the Institute becomes the Data Controller for that Personal Data.

Where a research student Processes Personal Data while working on a project led by a Institute research group, the Institute is the Data Controller.

Academic and academic-related staff must ensure that students they supervise are aware of the following:

A student should only use Personal Data for a Institute-related purpose with the knowledge and express consent of an appropriate member of academic staff (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course).

The use of Institute-related Personal Data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be Anonymized so that students are not able to identify the Data Subjects.

References

National Institute of Standards and Technology. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. January 16, 2020. Available from https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). Adopted April 27, 2016. Effective May 25, 2018. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Compliance and review

This Data Protection Policy will be regularly reviewed and updated to ensure its continued effectiveness and compliance with applicable data protection laws.

Failure to comply with this policy or its supporting standards, whether deliberate or due to careless disregard, will be treated as serious misconduct and may result in actions including (but not limited to) disciplinary action, dismissal, and civil and/or criminal proceedings.

This policy is reviewed on a periodic basis and updated as necessary by the Information Security and Privacy Office to ensure it remains accurate, relevant, and fit for purpose.

Staff Responsibilities:

All staff members are responsible for complying with this Data Protection Policy and handling personal data in a secure and confidential manner.

Staff will receive training and guidance on data protection principles and their responsibilities.

Breach Notification:

In the event of a personal data breach, PIMSAT will promptly assess the risk to individuals and, if required by applicable laws, report the breach to the relevant supervisory authority and affected individuals.

Contact Information:

For any inquiries or concerns regarding data protection or to exercise data subject rights, individuals can contact PIMSAT at the provided contact information.

By implementing this Data Protection Policy, PIMSAT is committed to maintaining the confidentiality, integrity, and security of personal data, ensuring compliance with applicable data protection laws, and fostering trust and confidence among our stakeholders.

Policy Revisions and History

Responsible Official:	Data Protection Officer	**Approval Authority:**	Ractor
Policy Number:	V. 3.5.0	**Effective Date:**	May 2022
Revision History:	• V. 3.4.3.1 approved September 18, 2020 • V. 3.4.3.2 effective July 1, 2018 • V. 3.4.3.3 effective July 1, 2017 • V. 3.4.3.4 approved July 13, 2017 • V. 2.7.5/V. 3.4.3.5 approved February 7, 2016 • V. 2.7.6 effective July 9, 2015		