AISCT
AMERICAN INTERNATIONAL SCHOOL OF CAPE TOWN

42 Soetvlei Avenue, Constantia 7806, Cape Town, South Africa
Tel +27 21 713 2220 **Email** aisct@aisct.org **Web** www.aisct.org

PROTECTION OF PERSONAL INFORMATION POLICY

1. INTRODUCTION

The right to privacy is an important human right entrenched and protected by the Constitution of the Republic of South Africa, 1996 and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). The American International School of Cape Town recognizes the importance of privacy and is committed to handling personal information in accordance with POPIA's provisions.

POPIA aims to protect the privacy of individuals through guiding principles which must be applied to the processing of personal information in a context sensitive manner. This gives effect to a person's constitutional right to privacy, which comprises of control over his or her personal information and being able to conduct his or her affairs without unwarranted intrusions.

This is the Privacy and Information Policy of the American International School of Cape Town ("AISCT") situated at 42 Soetvlei Avenue, Constantia 7806, Cape Town, South Africa.

AISCT is a non-profit educational institution providing educational services to students from kindergarten to high school level. Through the provision of these services the AISCT is by necessity involved in processing personal information of students, parents, guardians, applicants, employees, third party service providers and other stakeholders.

AISCT has the right to amend this Policy at any time with its unilateral decision. The data subject accepts the amended rules of the policy by becoming aware of its contents.

2. DEFINITIONS

2.1. Personal Information

Any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person or juristic person (e.g. a company) including, but not limited to, the following:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, color, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth;
- medical, financial, criminal or employment history of a person;
- any identifying name, number, symbol, email address, physical address, telephone number, location information, online identifier;
- biometric information of the person;
- personal opinions, views or preferences of a person, or of another person about the person;
- correspondence of a private or confidential nature, whether implicit or explicit, or would reveal the contents of original correspondence;

2.2. Data Subject

Natural or juristic person to whom the personal information relates.

2.3. Responsible Party

The entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information.

2.4. Operator

A person or entity processing personal information for a responsible party in terms of a contract or mandate, such as a third party service provider.

2.5. Information Officer

The Information Officer ensures compliance with POPIA. In the absence of a formally appointed Information Officer, the head of the organization is automatically responsible for performing the duties of the Information Officer.

The Information Officer must be registered with the South African Information Regulator established under POPIA, as soon as possible. Deputy Information Officers can also be appointed to assist the Information Officer in his or her duties.

2.6. Processing

Any activity or any set of operations, whether by automatic means or otherwise, concerning personal information and includes:

collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use; transmission, distribution or making available in any other form; merging, linking, restriction, degradation, erasure or destruction of information.

2.7. Record

Recorded information in any form, including:

Writing, tape recorder, computer equipment (hardware/software), or other electronic device from which information may be stored, derived, produced or recorded; label, marking, book, map, plan, graph, drawing, photograph, film, negative, tape, or any other device in which a visual image may be embodied and reproduced.

2.8. Filing System

Any structured set of personal information, in a centralized, decentralized or dispersed basis, which is arranged according to specific criteria.

2.9. Unique Identifier

Any identifier used by a responsible party which uniquely identifies that data subject in relation to that responsible party.

2.10. Consent

Voluntary, specific, informed expression of will in terms of which permission is given to process personal information.

2.11. Direct Marketing

Communication with a data subject for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or requesting the data subject to make a donation of any kind for any reason.

2.12. Biometrics

A technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

2.13. Surveillance

The use of closed circuit television cameras (CCTV) to transmit images to monitor for the safety and security of persons and property.

3. POLICY PURPOSE AND SCOPE

AISCT is the responsible party for the processing of personal information provided via interactions with the school. This policy applies to all personal information processed by AISCT regardless of the location where the personal information is stored and regardless of the information subject.

The purpose of this policy is to protect AISCT from the compliance risks associated with processing of personal information, including:

Breaches of confidentiality; damage to reputation; failure to provide data subjects with a choice.

This policy entrenches AISCT's commitment to the right to privacy and protection of personal information through compliance with POPIA and reasonable best industry practice, as well as a culture of privacy in the institution. This is to be achieved via:

- internal controls;
- practices which provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate needs of AISCT;
- appointment of an Information Officer and where necessary Deputy Information Officers;
- awareness training and guidance to individuals who process personal information.

4. POLICY APPLICATION

This policy applies to the governing body, all employees and volunteers, all other persons acting on behalf of AISCT and is to be read in conjunction with the provisions of POPIA.

5. RIGHTS OF DATA SUBJECTS

5.1. Right to Access Personal Information

A data subject has the right to obtain confirmation from AISCT as to whether personal information relating to them is being held and to access any such information held.

This may be done using the Personal Information Request Form obtainable from the Information Officer.

5.2. Right to Correction or Deletion of Personal Information

A data subject has the right to request necessary corrections of his or her personal information or to request deletion once AISCT is no longer authorized to retain the information.

5.3. Right to Object to Processing of Personal Information

A data subject may reasonably object to the processing of their personal information. AISCT will consider an objection against the requirements of POPIA plus any other applicable statutory and/or contractual record keeping requirements, and inform the data subject of their decision.

5.4. Right to Object to Direct Marketing

A data subject may object to the processing of their personal information for the purposes of direct marketing by means of unsolicited electronic communications.

5.5. Right to Complain to the Information Regulator

A data subject may submit a complaint to the Information Regulator if they feel any of their rights under POPIA have been infringed.

5.6. Right to be Informed

A data subject has a right to be informed that their personal information is being processed, and to be notified where there are reasonable grounds to believe their personal information has been accessed by an unauthorized person.

5.7. Right to Erasure

Upon request by the data subject, AISCT has the obligation to erase the data subject's personal information without undue delay if one the following applies:

- the personal information is no longer necessary for the purposes for which it was processed;
- the data subject withdraws consent to processing, and there is no other legitimate ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal information has been processed unlawfully;
- the personal information must be erased to comply with a legal obligation.

6. POLICY PRINCIPLES

6.1. Accountability

AISCT will ensure POPIA and the provisions of this policy are complied with through awareness training, building a culture of privacy, and encouraging desired behavior. AISCT undertakes to pursue appropriate action against individuals who through their actions and/or omissions, be it intentional or negligent, fail to comply with this policy.

6.2. Processing Limitation

Personal information processed under the control of AISCT will be processed in a fair, lawful, and limited manner, only with the consent of the data subject, and only for a specified purpose.

Consent will be obtained prior to processing of personal information from the data subject. In the case of a minor student, the consent will be obtained from their parent/legal guardian.

The data subject is to be made aware that their personal information may be shared with other entities (Department of Education, Google Classroom, etc.) by virtue of the nature of educational services.

6.3. Purpose Specification

AISCT will only process personal information for a specific purpose and/or legitimate reasons of which the data subject must be informed of prior to processing.

AISCT processes the following personal information of:

Students, including potential students who have applied for admission; alumni; parents and/or legal guardians of students; job applicants; all employees and volunteers; board members; third party service providers and external suppliers; any person visiting the website; any person visiting AISCT premises; any person whose image or vehicle is recorded through surveillance camera; other stakeholders.

The purpose for such processing being:

6.3.1. Students: provision of educational services; maintaining class registers and other requirements prescribed by and applicable legislation and statutory bodies; effective educational activities; building a school community.

6.3.2. Parents/Legal guardians: maintaining records as prescribed by statutory bodies and applicable legislation; contacting parent/legal guardian in case of necessity; legitimate communications; accounting and fees; building a school community.

6.3.3. Alumni: to preserve results and documents necessary to enroll into higher education institutions; keeping in touch regarding alumni events and maintaining contact; building a school community.

6.3.4. Applicants: sufficient application and evaluation process; informing the applicant of outcome.

6.3.5. Employees: assessment and hiring suitable and qualified staff; taxation, obligations prescribed by relevant legislation; to supply service providers with required information to operate benefits offered as part of remuneration; employment contract relationships; to assist teachers and/or other staff with official procedures; building a school community.

6.3.6. Board members: for recording who the board members are and other requirements prescribed by applicable legislation; entering into and maintaining board membership; for appointment and removal of board members.

6.3.7. Service providers: entering into and maintaining contractual relationships, keeping contact and ensuring performance; exercising potential claims after the expiry of the contract.

6.3.8. Persons visiting the website: technical operation of the website; enabling contact with AISCT.

6.3.9. Visitors to AISCT premises: ensuring safety of persons and property.

6.3.10. For surveillance camera (CCTV): ensuring the safety of employees, learners, parents/guardians and property.

AISCT maintains a legitimate basis for which all personal information is processed and will not process personal information if there is no legal obligation and/or legitimate interest and/or consent.

6.4. Further Processing Limitation

AISCT will not process information for another purpose unless that purpose is directly relatable to the original purpose. Should this be necessary it will only be done with the consent of the data subject.

6.5. Information Quality

AISCT will take reasonable steps to ensure that all personal information is complete, accurate and not misleading. Effort to ensure information quality will be context-sensitive, with greater effort where accuracy is of greater importance.

The data subject is responsible for the correct provision of their personal information.

If personal information is received from a third party, reasonable steps will be taken to confirm the accuracy of the information directly with the data subject or authorized sources.

6.6. Open Communication

AISCT will reasonably ensure that data subjects are aware that their personal information is being collected and the purpose for which it is being processed.

A 'Contact Us' facility is available on AISCT's website for data subjects who wish to submit queries or complaints regarding their personal information. Queries made using this facility will be redirected and marked for the attention of the Information Officer.

6.7. Security Safeguards

AISCT will ensure personal information is adequately protected by means of a secure filing system, with security measures to minimize risk of loss, unauthorized access, disclosure, interference, modification or destruction. The more sensitive the personal information, the greater the security.

Security measures will be regularly reviewed and tested to prevent unauthorized access and to combat cyber-attacks on IT networks.

All employment contracts will contain terms for use and storage of personal information; as well as confidentiality clauses to address the risk of unauthorized disclosures of personal information.

Service agreements will only be concluded with parties who are committed to lawful processing of personal information.

6.8. Data Subject Participation

A data subject is entitled to request the correction or deletion of their personal information under the control of AISCT by submitting a request to the Information Officer.

6.9. Transferring Personal Information

Personal information will only be transferred where there is consent, a legal obligation, in the performance of services by, or pursuit of a legitimate interest of, AISCT.

AISCT uses third party software for educational and administrative purposes and personal information may be hosted on the servers of those service providers. These service providers provide their own services and make their own decisions on what types of personal information they process for their own purposes. AISCT exercises caution in selecting service providers, and carefully considers the risk of processing personal information.

7. DUTIES AND RESPONSIBILITIES

7.1. Information Officers

AISCT has an appointed Information Officer. If necessary, additional Deputy Information Officers may be appointed to assist the Information Officer.

The Information Officer is responsible for:

- reasonable compliance with POPIA and is responsible for personal information processing activities of AISCT in general;
- keeping the governing body updated about the organization's information protection responsibilities in terms of POPIA;
- regularly analyzing privacy trends and regulations and aligning AISCT procedures with them;
- scheduling and conducting regular POPIA audits;
- being a convenient contact point to data subjects wanting to exercise their rights in terms of POPIA;
- approving contracts which may have an impact on personal information under the control of AISCT and overseeing the amendment of AISCT's employment contracts and service level agreements;
- ensuring all staff and persons acting on behalf of AISCT are aware of processing risks, this policy and security procedures;
- organizing and overseeing the awareness training of employees;
- working with the South African Information Regulator.

7.2. Governing Body

The governing body of AISCT cannot delegate its accountability and remain ultimately answerable for ensuring that legal obligations to comply with POPIA are met. They may however delegate their responsibility to capable individuals.

The governing body must ensure:

- an Information Officer is appointed and, if necessary, Deputy Information Officers;
- all persons processing personal information on behalf of AISCT are trained and aware of their obligation to protect personal information they come into contact with;
- awareness that a willful or negligent breach of this policy may result in disciplinary action or other appropriate sanction;
- scheduling of POPIA audits to review how AISCT processes personal information.

7.3. IT Director

AISCT's IT Director is responsible for ensuring:

- IT infrastructure and any other devices used for processing personal information meet reasonable security standards;
- all electronic personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- servers containing personal information are kept in a secure location, away from general access;
- all electronic personal information is backed-up and tested regularly;
- all back-ups are protected from unauthorized access, accidental deletion and malicious shacking attempts;
- all electronic transfers of personal information are encrypted;
- all servers, computers, iPads and other such devices containing personal information are protected by a firewall and up-to-date security software.

The IT Director is to perform regular IT audits to determine if electronically stored information has been accessed or acquired by any unauthorized persons, and ensure the proper functioning of hardware and software systems.

7.4. Employees and Others Processing on Behalf of AISCT

All employees and other persons processing personal information on behalf of AISCT ("persons") will, during the course of their employment or performance of services, gain access to personal information under the control of AISCT. These persons are required to treat personal information with the utmost care and confidentiality, and are to respect the privacy of data subjects.

Persons may not directly or indirectly disclose any part of personal information to the public, another unauthorized person or third party, either within or outside the organization, unless the information is already publicly known, or the disclosure is necessary to perform his/her duties or fulfil a lawful obligation.

Persons must request clarification from the Information Officer if there is any uncertainty about any aspect related to the protection of personal information.

Persons may only process information in the following circumstances:

- the data subject, or their parent/legal guardian, has consented;
- processing is necessary for the performance of duties or provision of services by the responsible party;
- a legal obligation on the responsible party;
- pursuit of a legitimate interest by the responsible party.

Persons will under no circumstances:

- process personal information which is not required to perform their work-related tasks or duties;

- save copies of personal information directly to their own private computers, laptops, tablets or mobile devices;
- share personal information informally or by means of unencrypted electronic communications (email, text message, etc.);
- transfer personal information without the express permission of the Information Officer.

Persons are responsible for:

- taking sensible precautions to keep all personal information they come into contact with secure;
- keeping areas where personal information may be found organized and to a minimum, with all confidential information out of view from unauthorized persons at all times;
- ensuring personal information is encrypted prior to transmitting electronically (the IT Director will assist where required);
- making sure all computers, laptops, tablets, mobile devices, flash drives and any other device containing personal information is password protected and never left unattended where it may be accessed by an unauthorized person. Passwords must be changed regularly and never shared with unauthorized persons or stored as plain-text;
- switching off devices or locking the screen when not in use (external drives, CDs, DVDs and other removable storage devices must be locked away when not in use);
- undergoing and taking proper note of awareness training provided to them;
- ensuring personal information is never discussed in public areas or with unauthorized individuals.

Should a person suspect or be aware of any security breach or breach of this policy, they must immediately report it to the Information Officer.

8. RETENTION PERIOD

Personal information under the control of AISCT is kept for the following periods:

8.1. Applicants: until a decision is made regarding the application.

8.2. Students: academic records shall be maintained indefinitely. Admission records and other such documents shall be retained for 20 years.

8.3. Parents/Legal guardians: 5 years after the student has left the school or 1 year after full payment of any outstanding monies owing to AISCT, whichever is longer.

8.4. Employees: information shall be retained for as long as is necessary for the performance of the employment contract, except for information whose retention period is otherwise specified, plus a further 5 years after the expiry of the contract.

8.5. Board members: for as long as processing is necessary for the performance of the contract pertaining to board membership; a further 5 years after the expiry of the contract.

8.6. Service providers: as long as is necessary for the performance of the contract; a further 5 years after the expiry of the contract.

8.7. Website visitors: only as long as is necessary for the technical operation of the AISCT website.

8.8. Visitors to the school: within 5 years.

Where personal information is provided by consent, and is not subject to any other legitimate interest or statutory obligation, the information shall be retained until consent is withdrawn or for 5 years, whichever is the shorter.

9. BREACH

In the event of a breach, the Information Officer notifies:

- The Information Regulator
- The data subject(s)

Notification must be carried out as soon as reasonably possible, at least within 72 hours, after having become aware of the breach.

The notification must contain all the relevant information concerning the breach. The Information Officer must remain available to provide further information and respond to queries of the data subject or the Information Regulator.

AISCT must pursue all reasonable efforts to solve the problem and secure the breach as fast as possible, as well as to prevent any further breach.

10. REMEDIES

A data subject may exercise their rights by contacting the Information Officer, all requests must be handled within a reasonable time.

10.1. Complaints Procedure

Complaints must be submitted in writing on the prescribed POPIA Complaint Form which can be obtained from the Information Officer, who will provide written acknowledgement of receipt within 3 working days.

The Information Officer will determine the nature of the complaint and whether it may have a wider impact on data subjects.

The Information Officer will consider the complaint and endeavor to resolve the complaint in accordance with the principles of POPIA, amicably and in a fair manner. The Information Officer will revert with a proposed remedy or dismissal, including reasons, within 10 working days of receipt of the complaint.

If a data subject is of the opinion that their complaint was not handled properly, or they believe that their rights have been abused, they may contact the South African Information Regulator or a court with jurisdiction for relief.

The Information Regulator of South Africa
SALU Building, 316 Thabo Sehume Street,
PRETORIA
Telephone: 012 406 4818
Fax: 086 500 3351
E-mail: inforeg@justice.gov.za
Website: www.justice.gov.za/inforeg