

**INTERNATIONAL SCHOOL OF CAPE TOWN (PROPRIETARY) LIMITED**

(Registration No. 2002/026764/07)

(hereafter "**ISCT**")

**POPIA POLICY**

**(in terms of the Protection of Personal Information Act 4 of 2013)**

Woodland Heights • 4 Edinburgh Close • Claremont • 7708 • Cape Town • South Africa • T +27 21 761 6202  
Struben House • 31 Eden Road • Claremont • 7708 • Cape Town • South Africa • T +27 21 180 4240  
W [www.isct.co.za](http://www.isct.co.za) • E [info@isct.co.za](mailto:info@isct.co.za)

**Table of Contents**

**Page No.**

1. INTRODUCTION .....	3
2. DEFINITIONS .....	4
3. OUR UNDERTAKINGS TO OUR USERS .....	11
4. CATEGORIES OF DATA SUBJECTS AND RECIPIENTS OF PERSONAL INFORMATION RELATING THERETO .....	13
5. HOW PERSONAL INFORMATION IS COLLECTED .....	14
6. WITHHOLDING OR WITHDRAWING CONSENT TO COLLECT AND PROCESS PERSONAL INFORMATION .....	16
7. SECURITY MEASURES & SAFEGUARDS .....	18
8. SECURITY BREACHES .....	20
9. DATA SUBJECT REQUESTING RECORDS .....	21
10. THE CORRECTION, DESTRUCTION OR DELETION OF PERSONAL INFORMATION .....	23
11. SPECIAL PERSONAL INFORMATION .....	23
12. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN .....	24
13. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION .....	24
14. DISCLOSURE AND TRANSFER OF PERSONAL INFORMATION TO THIRD PARTIES .....	25
15. TRANSBORDER INFORMATION FLOWS .....	26
16. ACCEPTANCE .....	27
17. RETENTION, ARCHIVING AND DESTRUCTION OF PERSONAL INFORMATION .....	27
18. DIRECT MARKETING .....	28
19. LINKS TO OTHER WEBSITES .....	29
20. OFFENCES AND PENALTIES .....	29
21. INFORMATION OFFICER .....	29
22. REVISION HISTORY .....	30

## 1. INTRODUCTION

- 1.1 The Responsible Party is the International School of Cape Town (Proprietary) Limited ("ISCT").
- 1.2 ISCT was established in 1998 and is a private co-educational school offering a respected British-style education through its Cambridge IGCSE Extended curriculum. As part of its business activities, ISCT collects and processes Personal Information.
- 1.3 The Protection of Personal Information Act of 2013 ("**POPIA**") is the central piece of legislation that regulates the lawful collection, storage, use, handling, processing, transfer, retention, archiving and disposal of a person's Personal Information.
- 1.4 ISCT is responsible to collect, store, use, handle, process, transfer, retain, archive, and otherwise manage Personal Information in a lawful, legitimate, and responsible manner and in accordance with the provisions set out in POPIA.
- 1.5 This POPIA Policy sets out, in general, how, and why ISCT collects and processes Personal Information, as well as the policies and procedures in place to ensure compliance with POPIA. This POPIA Policy document is available on request from ISCT's Information Officer, as well as on ISCT's website.
- 1.6 In compliance with POPIA, ISCT is committed to processing the Personal Information of Data Subjects lawfully and in a reasonable manner. ISCT will take reasonable and appropriate measures to accurately record a Data Subject's Personal Information as provided by them or their representatives and make reasonable efforts to ensure that Personal Information is complete, accurate and not misleading.
- 1.7 All employees, independent contractors, and representatives of ISCT are required to adhere to this POPIA Policy. Any external service provider responsible for providing and managing information technology to ISCT must adhere to the same information security principles contained in this POPIA Policy, or as are sufficient to

comply with POPIA, so as to ensure security measures are in place in respect of processing of Personal Information.

## 2. DEFINITIONS

2.1 In this Policy, the following words shall, unless otherwise stated or inconsistent with the context in which they appear, bear the following meanings and other words derived from the same origins as such words (that is, cognate words) shall bear corresponding meanings:

- |       |                           |  |
|-------|---------------------------|--|
| 2.1.1 | <b>"Aggregated Data"</b>  | in relation to Personal Information of a Data Subject, means de-identified Personal Information;                                   |
| 2.1.2 | <b>"Data Subject"</b>     | means the person to whom Personal Information relates;   |
| 2.1.3 | <b>"de-identify"</b>      | in relation to Personal Information of a Data Subject, means to delete any information that -                                      |
|       | 2.1.3.1                   | identifies the Data Subject;   |
|       | 2.1.3.2                   | can be used or manipulated by a reasonably foreseeable method to identify the Data Subject; or                                     |
|       | 2.1.3.3                   | can be linked by a reasonably foreseeable method to other information that identifies the Data Subject;                            |
| 2.1.4 | <b>"direct marketing"</b> | means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of - |

		2.1.4.1	promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or
		2.1.4.2	requesting the Data Subject to make a donation of any kind for any reason;
2.1.5	<b>"Information Officer"</b>		of, or in relation to, a private body means the head of a private body as contemplated in section 1, of PAIA;
2.1.6	<b>"Information Regulator"</b>		means the independent regulatory body having jurisdiction throughout South Africa, and having been established in terms of section 39 of POPIA to perform certain functions under both POPIA and PAIA;
2.1.7	<b>"ISCT"</b>		means the International School of Cape Town (Proprietary) Limited, registration number 2002/026764/07, a private company duly incorporated and registered in accordance with the laws of the Republic of South Africa;
2.1.8	<b>"operator"</b>		means a person who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
2.1.9	<b>"Personal Information"</b>		means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -



- |         |  |
|---------|--|
| 2.1.9.1 | information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, and birth of the person; |
| 2.1.9.2 | information relating to the education or the medical, financial, criminal or employment history of the person;   |
| 2.1.9.3 | any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;  |
| 2.1.9.4 | the biometric information of the person;   |
| 2.1.9.5 | the personal opinions, views, or preferences of the person;  |
| 2.1.9.6 | correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would  |

		reveal the contents of the original correspondence;
	2.1.9.7	the views or opinions of another individual about the person; and
	2.1.9.8	the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person;
2.1.10	<b>"Policy"</b>	means the policy recorded herein, being ISCT Policy on the Protection of Personal Information Act 4 of 2013;
2.1.11	<b>"processing"</b>	means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including –
	2.1.11.1	the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval,
	2.1.11.2	alteration, consultation, or use;
	2.1.11.3	dissemination by means of transmission, distribution or making available in any other form; or
	2.1.11.4	merging, linking, as well as restriction, degradation,



erasure, or destruction of information;

- 2.1.12      **"Promotion of Access to Information Act"** and **"PAIA"**      means the Promotion of Access to Information Act 2 of 2000, together with Regulation 187 of 15 February 2002 as amended on 1 June 2007;
- 2.1.13      **"Protection of Personal Information Act"** and **"POPIA"**      means the Protection of Personal Information Act 4 of 2013, together with any and all Regulations that may in the future be promulgated thereunder;
- 2.1.14      **"public record"**      means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body;
- 2.1.15      **"record"**      means any recorded information –
- 2.2.1.1      regardless of form or medium, including any of the following:
- 2.2.1.1.1      writing on any material;
- 2.2.1.1.2      information produced, recorded, or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded, or stored;



	2.2.1.1.3	label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
	2.2.1.1.4	book, map, plan, graph, or drawing;
	2.2.1.1.5	photograph, image, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
	2.2.1.2	in the possession or under the control of a responsible party;
	2.2.1.3	whether or not it was created by a responsible party; and
	2.2.1.4	regardless of when it came into existence;
2.2.17	<b>"responsible party"</b>	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing Personal Information, in this document, being ISCT;



- 2.2.18      **"restriction"**      means to withhold from circulation, use or publication any Personal Information that forms part of a filing system, but not to delete or destroy such information;
- 2.2.19      **"special Personal Information"**      means Personal Information as referred to in section 26 of POPIA concerning –
- 2.3.1.1      the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or
- 2.3.1.2      the criminal behaviour of a Data Subject to the extent that such information relates to –
- 2.3.1.2.1      the alleged commission by a Data Subject of any offence; or
- 2.3.1.2.2      any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings; and
- 2.3.2      **"unique identifier"**      means any identifier that is assigned to a Data Subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that Data Subject in relation to that responsible party;

### 3. OUR UNDERTAKINGS TO OUR USERS

- 3.1 Due to the nature of ISCT's business, we are necessarily involved in the collection, processing, and disclosure of Personal Information of a number of Data Subjects. Any person whose information ISCT collects, and processes is known as a "**Data Subject**" in this POPIA Policy.
- 3.2 ISCT undertakes to follow POPIA at all relevant times and to process Personal Information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of Data Subjects.
- 3.3 We undertake to process information only for the purpose for which it is intended, to enable us to do our work and perform our services, as agreed with Data Subjects.
- 3.4 ISCT may collect and process Personal Information for any legitimate purpose, including but not limited to:
- 3.4.1 conduct our business operations, as well as ensure the good upkeep, development, improvement and safeguarding of our business;
  - 3.4.2 carry out the vision, mission, and objective of ISCT;
  - 3.4.3 provide and maintain sound and professional services, including support to Data Subject as and when required;
  - 3.4.4 performance of a contract between ISCT and a Data Subject;
  - 3.4.5 comply with contractual obligations and legislative mandates;
  - 3.4.6 human resources and employment purposes such as: (1) recruitment, selection, and placement; (2) administration of compensation and benefits; (3) performance management and training; and (4) government reporting;
  - 3.4.7 risk management which includes physical and electronic security and access control;



- 3.4.8 planning; procurement of goods and services; and rendering of services;
- 3.4.9 notify Data Subjects of news, new products, special offers, services and/or developments within ISCT, as well as general information about other goods, services, and events which ISCT offers that are similar to the existing ISCT offerings, unless the Data Subject has opted out of receiving this information;
- 3.4.10 contact Data Subjects and/or their representatives by email, telephone call, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products, or contracted services, including security updates, when necessary or reasonable for their implementation;
- 3.4.11 confirm, verify, and update Data Subject's details;
- 3.4.12 maintain administrative and management systems, as well as reporting thereon;
- 3.4.13 generate, in aggregated form, statistics and data to develop strategic and marketing plans;
- 3.4.14 assist ISCT in future dealings with Data Subjects;
- 3.4.15 evaluate or conduct a merger, divestiture, restructuring, reorganisation, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us about Data Subjects is among the assets transferred;
- 3.4.16 comply with any legal and/or regulatory requirements,  
  
all of which are collectively termed the "**ISCT Purpose**".
- 3.5 Whenever necessary, ISCT shall obtain consent to process Personal Information.

#### 4. CATEGORIES OF DATA SUBJECTS AND RECIPIENTS OF PERSONAL INFORMATION RELATING THERETO

- 4.1 The following table sets out the categories of Data Subjects, the categories of Personal Information relating thereto which are processed by ISCT, and the recipients of the Personal Information.

CATEGORIES OF DATA SUBJECTS	PERSONAL INFORMATION THAT MAY BE PROCESSED	RECIPIENTS
Prospective and current parents / legal guardians	name, identity number, biographical information, contact details, physical and postal address, employment details	Only for internal use. No sharing of information.
Prospective and current learners	name, identity number, biographical information, contact details, academic history, medical information, nutritional information	Department of Education
Prospective and current employees, consultants, contractors, interns, and volunteers	name, identification number, biographical information, contact details; educational, employment and criminal history, biometric and health information, psychometric assessments and references, background checks, account information, performance reports and skills/training reports	Only for internal use. No sharing of information.
Service Providers	name, company registration number / identity number, biographical information, physical and postal address, authorised signatories,	Only for internal use. No sharing of information.

	contact details, compliments, or complaints	
--	---	--

## 5. HOW PERSONAL INFORMATION IS COLLECTED

5.1 Personal information is usually collected:

- 5.1.1 directly from a Data Subject or their representatives;
- 5.1.2 through electronic communications, meetings, telephone calls, and in general dealings with Data Subjects or their representatives;
- 5.1.3 by referring to a Data Subject's website and/or any social media and online profiles to collect Personal Information from these and other public platforms;
- 5.1.4 through monitoring activity on any of our IT and electronic networks, social media platforms and our website, and gathering information about who is visiting and using our website and how, in order to fulfil the ISCT Purpose.

5.2 We shall stop processing Personal Information if the required consent is withdrawn, or if a legitimate objection is raised.

5.3 We shall collect Personal Information directly from the Data Subject, or their representative, whose information we require, unless:

- 5.3.1 the information is of public record;
- 5.3.2 the Data Subject has consented to the collection of their Personal Information from another source;
- 5.3.3 the collection of the information from another source does not prejudice the Data Subject;
- 5.3.4 the processing of the information is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;

- 5.3.5 the information to be collected is necessary for the maintenance of law and order or national security;
- 5.3.6 the information is being collected to comply with a legal obligation, including an obligation to SARS;
- 5.3.7 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated;
- 5.3.8 the processing is necessary for pursuing the legitimate interests of ISCT or of a third party to whom the information is supplied.
- 5.3.9 where requesting consent would prejudice the purpose of the collection of the information; or
- 5.3.10 where requesting consent is not reasonably practical in the circumstances.
- 5.4 We shall retain records of the Personal Information we have collected for the minimum period as required by law unless the Data Subject has furnished their consent or instructed us to retain the records for a longer period.
- 5.5 We shall de-identify, destroy, or delete records of the Personal Information, as appropriate, as soon as reasonably possible after the time period for which we were entitled to hold the records has expired.
- 5.6 We shall restrict the processing of Personal Information:
  - 5.6.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;
  - 5.6.2 where the purpose for which the Personal Information was collected has been achieved and where the Personal Information is being retained only for the purposes of proof;



- 5.6.3 where the Data Subject requests that the Personal Information is not destroyed or deleted, but rather retained; and/or
- 5.6.4 where the Data Subject requests that the Personal Information be transmitted to another automated data processing system.
- 5.7 Once the processing of Personal Information has been restricted, the further processing of Personal Information shall only be undertaken:
  - 5.7.1 if the requirements of paragraphs 5.6.3 above have been met;
  - 5.7.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the Data Subject, or a third person;
  - 5.7.3 where the information is used for historical, statistical or research purposes and the identity of the Data Subject will not be disclosed; or
  - 5.7.4 where this is required by the Information Regulator appointed from time to time in terms of POPIA.
- 5.8 POPIA requires that all your Personal Information and related details as supplied are complete, accurate and up to date. Whilst ISCT will always use its best endeavours to ensure that your Personal Information is reliable, it is your responsibility to advise ISCT of any changes to your Personal Information, as and when these changes may occur.

## **6. WITHHOLDING OR WITHDRAWING CONSENT TO COLLECT AND PROCESS PERSONAL INFORMATION**

- 6.1 Data Subjects have the right to have Personal Information processed in accordance with the conditions of lawful processing of Personal Information as set out in POPIA.
- 6.2 Providing Personal Information is generally voluntary. Therefore, Data Subjects and their representatives are within their rights to withhold consent or to withdraw consent to ISCT collecting and processing their Personal Information.



- 6.3 ISCT reserves the right to decline to deal with any person who fails to provide Personal Information, withholds, or withdraws consent, or objects to the processing of Personal Information, which ISCT has requested and which ISCT deems necessary, in its sole discretion.
- 6.4 Should a Data Subject, or its representative, fail or refuse to provide Personal Information, the Personal Information will not be processed. The services provided by ISCT will therefore not be rendered in respect of the aforementioned Data Subject.
- 6.5 In the event that a Data Subject or its representative withdraws consent, ISCT may continue to process the Personal Information to the extent necessary to implement a contract with the Data Subject, or to protect the legitimate interests of the Data Subject, or to protect ISCT's legitimate interests, or to comply with any legal obligation.
- 6.6 In terms of section 11(3) of POPIA, and in the prescribed manner, Data Subjects or their representatives have the right, unless legislation provides for such processing, to object at any time to ISCT processing their Personal Information, on reasonable grounds and relating to their particular situation, where the processing is:
- 6.6.1 not covered by consent; and/or
  - 6.6.2 not necessary to discharge a legal obligation or protect ISCT's or the Data Subject's legitimate interests.
- 6.7 Upon receipt of notice of objection together with the reasons therefore, ISCT shall place any further processing of a Data Subject's Personal Information on hold until the reason for the objection has been addressed and either –
- 6.7.1 the objection is resolved and withdrawn; or
  - 6.7.2 the objection is upheld and accepted by ISCT.
- 6.8 In the event that the objection is upheld, no further processing of a Data Subject's Personal Information shall be done by ISCT.



- 6.9 In addition to a Data Subject's right to notify us of their objection to the processing of their Personal Information, Data Subjects have the right to lodge a complaint directly with the Information Regulator in terms of section 74 of POPIA, alleging interference with the protection of their Personal Information, at:

JD House, 27 Stiemens Street  
Braamfontein  
Johannesburg, 2001  
PO Box 31533  
Braamfontein, Johannesburg, 2017  
Tel: 010 023 5207  
Email: [complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za) / [infoereg@justice.gov.za](mailto:infoereg@justice.gov.za)

## 7. SECURITY MEASURES & SAFEGUARDS

- 7.1 All Personal Information, whether hard copy or a soft copy, which a Data Subject provides to ISCT will be held and stored safely and securely and for ISCT Purpose. ISCT will take reasonable and appropriate measures to keep Personal Information secure, although we cannot guarantee its absolute security.
- 7.2 The transmission of Personal Information is at the risk of the Data Subject or its representative. Once we have received Personal Information, we will use strict procedures and security features to try to prevent unauthorised access.
- 7.3 ISCT may store Personal Information physically and/or electronically (which may include cloud-based storage).
- 7.4 In order to ensure the security, integrity, and confidentiality of the Personal Information in ISCT's possession, and to protect it against loss or damage or unauthorised access, we implement the following security safeguards:
- 7.4.1 Where appropriate, hard copy archived files are stored behind locked doors and protected by access control.



- 7.4.2 Physical access points to ISCT's premises are limited with provision for physical security controls, such as window bars, grilles, shutters, and security doors. Where required access points are enhanced by the use of intruder detection systems, guard services and/or closed-circuit television surveillance;
- 7.4.3 Physical access is also controlled and monitored through a combination of manned guarding, electronic access control systems, ID access cards, visitor management systems, biometric activation doors;
- 7.4.4 All the user terminals on our internal computer network and our servers are protected by passwords which are changed on a regular basis;
- 7.4.5 Agreements concluded with third parties / service providers include the protection of confidentiality of information;
- 7.4.6 Risks are assessed during the development of new applications and systems, when changing existing systems, when changing business processes and when areas of concern are identified;
- 7.4.7 Risk to our information and communication technology ("ICT") infrastructure, networks and systems is managed through vulnerability and threat testing and awareness, audit controls, incident management and security awareness training. Similar safeguards are required from service providers, suppliers and business partners who require access to personal information collected by ISCT;
- 7.4.8 Vulnerability assessments are carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place;
- 7.4.9 We use an internationally recognised Firewall to protect the records on our local servers, and we run antivirus protection at least every week to ensure our systems are kept updated with the latest patches;



- 7.4.10 Our staff are trained to carry out their duties in compliance with POPIA and this POPIA Policy;
  - 7.4.11 It is a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our Data Subject's affairs, including their Personal Information; and
  - 7.4.12 The digital work profiles and privileges of staff who have left our employ are properly terminated.
- 7.5 These security safeguards are verified on a regular basis to ensure effective implementation, and these safeguards are continually updated as is necessary in response to new risks or deficiencies.

## 8. SECURITY BREACHES

- 8.1 Should it be found that the Personal Information of a Data Subject which we are retaining has been accessed and/or acquired by an unauthorised person, we shall:
  - 8.1.1 determine the scope of the compromise/breach;
  - 8.1.2 restore the integrity of our information system;
  - 8.1.3 notify the Information Regulator of such breach; and
  - 8.1.4 notify the affected Data Subject(s) or their representative(s) of such breach unless we are no longer able to identify and/or contact the affected Data Subject.
- 8.2 This notification will take place as soon as reasonably possible after the discovery of the compromise/breach.
- 8.3 Such notification shall be given in writing and shall first be given to the Information Regulator. Notification to the Data Subject shall only be delayed if a public body



responsible for the prevention, detection or investigation of offences, or the Information Regulator, determines it will impede a criminal investigation.

8.4 The notification to the Data Subject or their representative shall be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the Data Subject:

8.4.1 by mail to the Data Subject's last known physical or postal address;

8.4.2 by email to the Data Subject's last known email address;

8.4.3 by publication on our website or in the news media; or

8.4.4 as directed by the Information Regulator.

8.5 This notification to the Data Subject shall give sufficient information to enable the Data Subject to protect themselves against the potential consequences of the security breach, and shall include:

8.5.1 a description of the possible consequences of the breach;

8.5.2 details of the measures that we intend to take or have taken to address the breach;

8.5.3 the recommendation of what the Data Subject could and/or should do to mitigate the adverse effects of the breach; and

8.5.4 if known, the identity of the unauthorised person(s) who may have accessed, or acquired the Personal Information.

## 9. DATA SUBJECT REQUESTING RECORDS

9.1 On production of proof of identity, any person is entitled to request that we confirm whether or not we hold any Personal Information about that person in our records, as well as to request that we provide:





- 9.1.1 the details of any of your Personal Information that ISCT holds, including any record relating to the respective Data Subject's Personal Information;
- 9.1.2 the details of the manner in which ISCT has used and processed the respective Data Subject's Personal Information; and/or
- 9.1.3 information about any third parties or categories of third parties who have or have had access to the respective Data Subject's Personal Information.
- 9.2 Such request shall be made in writing and submitted to ISCT's Information Officer. The requester shall make the request in terms of section 53 of PAIA, and specifically as set out in the relevant Form annexed to ISCT's PAIA Manual, alternatively as set out in Form C of the PAIA Regulations of 2002 as amended.
- 9.3 We shall comply with such request within a reasonable period of time, in a reasonable manner and in an understandable form.
- 9.4 In certain circumstances, we will be obliged to refuse to disclose the record containing the respective Data Subject's Personal Information. In other circumstances, we will have discretion as to whether or not to do so.
- 9.5 In all cases where the disclosure of a record will entail the disclosure of information that is additional to the Personal Information of the Data Subject requesting the record, the written consent of the Information Officer (or his/her delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of PAIA.
- 9.6 If a request for Personal Information is made and part of the requested information may, or must be refused, every other part shall still be disclosed.
- 9.7 The aforementioned clauses are to be read in conjunction with ISCT's PAIA Manual, accessible on ISCT's website.



## 10. THE CORRECTION, DESTRUCTION OR DELETION OF PERSONAL INFORMATION

- 10.1 Data Subject's or their representatives are entitled to request us, where necessary, to correct or delete their Personal Information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.
- 10.2 Data Subject's or their representatives also have the right to request us to destroy or delete records of their Personal Information that we are retaining.
- 10.3 Such request shall be made in writing and submitted to ISCT's Information Officer.
- 10.4 On receiving either of the requests as set out above, ISCT shall follow the process as set out in section 24 of POPIA, and shall alter, substantiate, or destroy their records, as soon as reasonably practicable.
- 10.5 In the event that a dispute arises regarding a Data Subject's rights to have information corrected, and in the event that the Data Subject so requires, ISCT will attach to the information, in a way that it will always be read with the information, an indication that the correction of the Personal Information has been requested but has not been made.
- 10.6 Should a Data Subject or their representative request us to correct, delete or destroy their Personal Information, we shall notify them of the action we have taken as a result of the request.

## 11. SPECIAL PERSONAL INFORMATION

- 11.1 Special rules apply to the collection and use of special Personal Information, which information relates to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.
- 11.2 In certain circumstances, ISCT may collect certain special Personal Information about a Data Subject in order to fulfil the ISCT Purpose. As the processing of special

Personal Information requires higher levels of protection, ISCT has implemented appropriate safeguards to process such special Personal Information.

- 11.3 In terms of section 27(1)(a) of POPIA, we shall not process any of this special Personal Information without having obtained your consent. On rare occasions there may be other reasons for processing your special Personal Information, such as where this is necessary for the establishment, exercise, or defence of a right or an obligation in law or where such information has been deliberately made public by you.

## **12. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN**

- 12.1 In order to fulfil the ISCT Purpose and carry out ISCT's line of business and objectives, ISCT processes Personal Information of children on a daily basis.
- 12.2 ISCT only processes Personal Information of children as aforementioned if we have the consent of the child's parent or legal guardian.

## **13. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION**

- 13.1 In the following circumstances, ISCT will require prior authorisation from the Information Regulator before processing any Personal Information:
- 13.1.1 in the event that ISCT intends to utilise any unique identifiers of Data Subjects (account numbers, file numbers or other numbers or codes allocated to Data Subjects for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;
- 13.1.2 if ISCT is processing information on criminal behaviour or unlawful or objectionable conduct;
- 13.1.3 if ISCT is transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

- 13.2 The Information Regulator will be notified of our intention to process any personal information as set out in paragraph 13.1 above prior to any processing taking place and we shall not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 (four) weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which period must not exceed 13 (thirteen) weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

#### **14. DISCLOSURE AND TRANSFER OF PERSONAL INFORMATION TO THIRD PARTIES**

- 14.1 To carry out ISCT Purpose, ISCT's owners, managers, employees, consultants, and contractors will need to review, consider, verify, and discuss the Personal Information collected. In addition, we may share Personal Information with ISCT's affiliates, which include ISCT's holding company, and any other subsidiaries, joint venture partners, other entities which we control or that are under common control with us, or our business partners.
- 14.2 To carry out ISCT Purpose, ISCT may transfer and/or disclose Personal Information to third parties, which may include approved third party product and service providers, suppliers and related companies or agents, as well as third party contractors, subcontractors, and/or their subsidiaries and affiliates. Examples of third party contractors ISCT uses are providers of IT services, website management, data backup, security, and cloud storage.
- 14.3 ISCT may also disclose a Data Subject's Personal Information to third parties where necessary to carry out the services or activities requested of ISCT, or to protect ISCT or the Data Subject's legitimate interests, including where the transfer and/or disclosure is necessary for ISCT to perform in terms of a contract or for the implementation of pre-contractual measures taken in response to a request from the Data Subject.

- 14.4 ISCT may also disclose a Data Subject's Personal Information to third parties for research and statistical purposes. In this regard, ISCT will ensure that the Personal Information is de-identified prior to such disclosure and/or transfer to the respective third parties and that only Aggregated Data is transferred.
- 14.5 The aforementioned disclosure/s shall always be subject to a written agreement and/or undertaking concluded between ISCT and such third party, obligating the third party to comply with strict confidentiality, with all the information security conditions and provisions as contained in this POPIA Policy and/or as contained in POPIA itself, unless ISCT informs the Data Subject otherwise before such transfer and/or disclosure.
- 14.6 Where required by law, some or all of the Personal Information collected by ISCT may be disclosed to any governmental authority or regulatory body.
- 14.7 In the event that there is a change of corporate ownership within ISCT, the new owners shall be provided with our files, including any and all information collected. In addition, we may share or transfer Personal Information in connection with, or during negotiations of, any merger, sale of ISCT assets, financing, or acquisition of all or a portion of our business to another company or entity.

## 15. **TRANSBORDER INFORMATION FLOWS**

ISCT may not and shall not transfer a Data Subject's Personal Information to a third party in a foreign country, unless:

- 15.1 the Data Subject consents to the disclosure and/or transfer, or requests it; or
- 15.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the Personal Information in a manner similar to POPIA, and such third party is governed by similar rules which prohibit the onward transfer of the Personal Information to a third party in another country; or
- 15.3 the disclosure and/or transfer of the Personal Information is required for the performance of the contract between ISCT and the Data Subject, or is necessary

for the implementation of precontractual measures taken in response to a request from the Data Subject; or

- 15.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the Data Subject entered into between ISCT and the foreign third party; or
- 15.5 the disclosure and/or transfer of the Personal Information is for the benefit of the Data Subject, and it is not reasonably possible to obtain their consent and that if it were possible, the Data Subject would be likely to give such consent.

## 16. **ACCEPTANCE**

Data Subjects consent to the collection, processing, disclosure, storage, and general treatment of Personal Information described in this POPIA Policy, and as may be necessary to fulfil the ISCT Purpose, by:

- 16.1 signing ISCT's POPIA consent form;
- 16.2 agreeing to and/or accepting ISCT's POPIA Policy;
- 16.3 dealing with ISCT after being advised of ISCT's terms of engagement or this POPIA Policy; or
- 16.4 by providing ISCT, or permitting ISCT to be provided with, their Personal Information in order for ISCT to carry out any service or legitimate activity.

## 17. **RETENTION, ARCHIVING AND DESTRUCTION OF PERSONAL INFORMATION**

- 17.1 The POPIA principle that Personal Information is not retained for longer than is necessary for achieving the purpose for which it was collected and subsequently processed, is one by which ISCT abides.
- 17.2 The exceptions to the above principle specifically provided in POPIA are where –
  - 17.2.1 the retention of the record is required or authorised by law;



- 17.2.2 ISCT reasonably requires the record for lawful purposes related to its functions or activities;
- 17.2.3 the retention of the record is required in terms of an agreement between ISCT and the Data Subject; and/or
- 17.2.4 the record is retained for historical purposes, with ISCT having established appropriate safeguards against the record being used for any other purpose.
- 17.3 Subject to the aforementioned exceptions, all Personal Information shall be retained for a period of 8 (eight) years, unless consent is revoked earlier, or consent is provided in writing for further retention.
- 17.4 When ISCT is no longer authorised to retain a Data Subject's Personal Information, it shall destroy or delete such Personal Information or records of Personal Information, or de-identify them in a manner that prevents their reconstruction in an intelligible form.

## 18. DIRECT MARKETING

- 18.1 ISCT shall only carry out direct marketing (using any form of electronic communication) to Data Subjects where:
  - 18.1.1 ISCT obtained a Data Subject's Personal Information, more specifically their contact details, in the context of selling and/or providing its services to the Data Subject, and for the purpose of direct marketing of similar services and/or activities;
  - 18.1.2 the Data Subject was given an opportunity to object to receiving direct marketing material by electronic communication at the time that their Personal Information was collected; and
  - 18.1.3 the Data Subject did not object then or at any time after receiving any such direct marketing communications from ISCT.



- 18.2 All direct marketing communications shall disclose ISCT's name and shall contain an address or other contact details to which a request for communications to cease may be sent to.

## 19. LINKS TO OTHER WEBSITES

ISCT's website may, from time to time, contain links to third party websites. If a Data Subject follows a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. We do not exercise control over third party's privacy policies, and you should refer to the privacy policy of any such third party to establish how such third party protects your privacy before you submit any Personal Information to these websites.

## 20. OFFENCES AND PENALTIES

- 20.1 POPIA provides for serious penalties for the contravention of its terms. For minor offences, a guilty party can receive a fine or be imprisoned for up to 12 (twelve) months. For serious offences, the period of imprisonment rises to a maximum of 10 (ten) years. Administrative fines for ISCT can reach a maximum of R10 million.
- 20.2 Breaches of this POPIA Policy by ISCT's employees, contractors and/or representatives will be viewed by ISCT as a serious disciplinary offence and appropriate disciplinary measures shall follow.

## 21. INFORMATION OFFICER

- 21.1 ISCT's Information Officer details are:

Name : Katherine Reed  
Address : Woodland Heights, 4 Edinburgh Close, Claremont, Cape Town, 7806  
Email : popia@isct.co.za  
Telephone : +27 (21) 761 6202  
for the attention of the Information Officer.



21.2 The Information Officer's responsibilities include, amongst others:

21.2.1 ensuring compliance with POPIA;

21.2.2 dealing with requests which we receive in terms of POPIA; and

21.2.3 working with the Information Regulator in relation to investigations.

21.3 In carrying out their duties, our Information Officer and Deputy Information Officer ensure that:

21.3.1 this POPIA Policy is implemented;

21.3.2 this POPIA Policy is developed, monitored, maintained, and made available;

21.3.3 internal measures are developed and maintained together with adequate systems to process requests for information or access to information; and

21.3.4 copies of POPIA Policy are provided to persons at their request, hard copies to be provided upon payment of a fee (as set out in ISCT's PAIA Manual).

## 22. REVISION HISTORY

ISCT may update this POPIA Policy at any time by publishing an updated version on its website. When ISCT makes changes to this POPIA Policy, it will amend the revision date. The updated policy will apply from the effective date. We encourage you to review this policy regularly to remain up to date and informed.

VERSION	REVISION DATE	EFFECTIVE DATE
Version 1	November 2022	30 November 2022