



C O M P A N Y P O L I C Y

PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

Document Reference: 001

Revised Date	5 May 2026
Approved By	Dr Gerhard Botha (CEO)
Review Cycle	Every three (3) years
Status	Approved

TABLE OF CONTENTS

#	SECTION	PAGE
1	Purpose	3
2	Scope	3
3	Definitions	3
4	Personal Information	3
5	POPIA Principles	4
6	Collection of Information	4
7	Use of Information	4
8	Recipient for processing of Personal Information	5
9	Special Personal Information	5
10	Children's Information	5
11	Security Measures	5
12	Data Retention and Disposal	6
13	Data Subject Rights	6
14	Direct Marketing	6
15	Cross-border Transfers	6
16	Employee Responsibilities	7
17	Information Officer	7
18	Review	7

1. PURPOSE

This policy ensures that the organisation complies with the Protection of Personal Information Act, 4 of 2013 (POPIA) and protects all personal information processed by the company.

2. SCOPE

This policy applies to:

- All employees.
- Directors and management.
- Contractors and consultants.
- Suppliers processing information on ACRP's behalf.
- All systems, records, devices and platforms containing personal information.

3. DEFINITIONS

All terms not defined herein shall bear the same meaning as in applicable legislation. Key definitions include:

- **"Data subject"** – refers to the person to whom personal information relates.
- **"Information Officer"** – refers to the head of a private body as contemplated in PAIA.
- **"Personal information"** – refers to information relating to an identifiable, living person, or when applicable, a juristic person.
- **"Processing"** – refers to any activity or operation(s) concerning personal information (by automatic means or not), which can include collection, receipt, updating, merging, alteration, etc.
- **"PAIA"** – Promotion of Access to Information Act No. 2 of 2000.
- **"POPIA"** – Protection of Personal Information Act No.4 of 2013.
- **"Record"** – refers to any recorded information regardless of the form, including, for example, written documents, audio, digital and video materials. A record requested from a public or private body refers to a record that is in that body's possession regardless of whether that body created the record.

4. PERSONAL INFORMATION

Personal information includes, but is not limited to:

- Names and ID numbers
 - Contact details, addresses (physical/email)
 - Financial details
 - Employment records
 - Health information
 - Biometric data
-

-
- Information relating to race, gender, marital status, age, disability, religion, language, etc.
 - Customer and supplier records (including affiliate and service provider databases)
 - Correspondence revealing personal/ confidential information

5. POPIA PRINCIPLES

The organisation will ensure personal information is:

- 5.1 Collected lawfully and fairly;
- 5.2 Used only for legitimate purposes of the organisation;
- 5.3 Accurate and updated when required;
- 5.4 Kept only as long as necessary;
- 5.5 Protected against loss, misuse or unauthorised access;
- 5.6 Shared only when lawful and necessary;
- 5.7 Processed transparently.

6. COLLECTION OF INFORMATION

The organisation will collect personal information under different circumstances and may include the following, though not be limited to them:

- Directly from the individual where possible (through direct contact with ACRP, using our services, using our online platforms, etc.);
- With consent where required;
- From social media platforms;
- From service providers and other third parties;
- Only information necessary for the purpose of fulfilling the organisation's duties;
- With clear notice explaining why it is collected.

7. USE OF INFORMATION

Personal information may be used for:

- Employment administration
 - Operational purposes (including, but not limited to, affiliation registration, renewal notices, CPD event promotions, newsletters, general enquiries, etc.)
 - Contracts and billing
 - Legal compliance (for example for tax, FICA, QCTO, SAQA and NQF requirements)
 - Security and access control.
-

8. RECIPIENTS FOR PROCESSING PERSONAL INFORMATION

ACRP may provide Personal Information to service providers/third parties, for the efficient working of the organisation, and who render specific services, such as:

- Capturing, organising and storing of data;
- Correspondence with various stakeholders;
- Conducting of due diligence checks;
- Administrative support;
- Banking Institutions, Government Institutions or regulatory bodies (such as SAQA and QCTO), law enforcement agencies, etc.

All third parties are required to sign Confidentiality Agreements to ensure that they adhere to the requirements for keeping personal information confidential and using it only for its intended purpose.

9. SPECIAL PERSONAL INFORMATION

Special personal information (health, religion, race, biometrics, criminal history, etc.) will only be processed where legally permitted / required and with proper safeguards.

10. CHILDREN'S INFORMATION

Information relating to children will only be processed with consent of a competent person or where it is allowed by law.

11. SECURITY MEASURES

The organisation has taken every reasonable and affordable measure to keep personal information secure, confidential and protected. Some of these measures are:

- Password protection
- Access controls
- Secure storage
- Anti-virus and firewall protection
- Staff awareness training
- Incident reporting procedures
- Confidentiality Agreements

Though measures have been implemented to minimise threats, ACRP cannot guarantee that data breaches will not occur. Therefore, data subjects are encouraged to implement their own security measures as well.

Any suspected loss, theft or unauthorised access to personal information will be reported immediately to the relevant authorities. The organisation will investigate and notify affected parties where required.

12. DATA RETENTION AND DISPOSAL

Information will only be kept for as long as required by law or the organisation's needs, then securely destroyed or deleted, unless the destruction is delayed due to pending litigation, audits, government investigations or similar proceedings.

13. DATA SUBJECT RIGHTS

Individual registered affiliates of ACRP may request to:

- Access their information (or directly access their own profiles on the online database);
- Correct inaccurate information or update their contact information (or directly access their own profiles on the online database);
- Object to processing unless legislation provides for such processing;
- Withdraw consent where applicable;
- Request deletion where lawful;
- in the case of deletion of personal data, ACRP may need to terminate the affiliation as the data may be necessary to maintain the relationship;
- Requests for updating, correction or deletion of data must be made in writing using the prescribed forms (available from the ACRP office) and submitted to the Information Officer;
- ACRP retains the right to refuse the deletion of some personal information should it be required to maintain the affiliation relationship or other contracts.

14. DIRECT MARKETING

Electronic marketing will only occur where consent exists or where permitted by POPIA. Opt-out options must always be available.

15. CROSS-BORDER TRANSFERS

ACRP may only transfer personal information to a third party in another country where:

- The recipient is subject to laws, agreements, or rules that provide adequate protection similar to POPIA, including restrictions on further transfers;
 - The data subject has consented to the transfer;
 - The transfer is necessary for the performance of a contract with the data subject or to take pre-contractual steps at their request;
 - The transfer is required for a contract in the interest of the data subject; or
 - The transfer is for the benefit of the data subject, and consent cannot reasonably be obtained, but would likely have been given.
-

16. EMPLOYEE RESPONSIBILITIES

All employees must:

- Sign the ACRP Confidentiality Agreement
- Keep information confidential
- Follow security procedures
- Report breaches immediately to the Information Officer
- Use company systems responsibly
- Attend POPIA training when required

Failure to comply may lead to disciplinary action.

17. INFORMATION OFFICER

The organisation appoints an Information Officer responsible for POPIA compliance, training, complaints, and regulator communication. Contact details of the Information Officer and Deputy Information Officer can be found in the PAIA Manual, and they may be reached at the following email address: info@acrp.org.za.

18. REVIEW

This Policy will be reviewed annually or when legislation changes require a review.

Approved:

Chief Executive Officer	Signature	Date:
Dr Gerhard Botha		2026/05/05

This Policy was drafted and refined with the assistance of AI tools. All content was reviewed, edited and approved by the author to ensure compliance with applicable laws and the company's standards.