

**SOUTH AFRICAN MEDICAL
RESEARCH COUNCIL**



PERSONAL INFORMATION PRIVACY POLICY



Document review and approval

Revision history

Version	Author	Date
1	Legalese	October 2021
2	General Counsel	November 2021
3		
4		
5		
6		
7		

This document has been reviewed by

	Reviewer	Date reviewed
1	Executive Management Committee	November 2021
2	Audit, Risk & IT Committee	February 2022
3		
4		
5		
6		
7		

This document has been approved by

	Name	Date reviewed
1	Board: Chairperson (See Resolution)	February 2022
2		
3		
4		
5		

Contents

1. Important information and who we are
2. Role as "Responsibility Party" and/or "Operator"
3. Changes to the Private Policy and your Duty to Inform us of Changes
4. Third-Party Links on Website or otherwise
5. The data we collect about you and through what avenue
6. How is your personal data collected
7. How we use your personal data
8. Purpose for which we will use your personal data
9. Disclosures of personal data
10. Express cookies provision
11. International transfers
12. Data Security
13. Data Retention
14. Your legal rights
15. Glossary
16. Your legal rights

THE SOUTH AFRICAN MEDICAL RESEARCH COUNCIL'S PRIVACY AND PERSONAL INFORMATION POLICY

The South African Medical Research Council (“SAMRC”) adheres to the highest standards of protecting your personal information as a member, affiliate, staff member or any other data subject when we process it by virtue of your use of our services, our website <https://www.samrc.ac.za/> or any of its related blogs, websites, applications or platforms (collectively, “the Website”), or by providing us with your personal information in any other way such as being a partner with us or a contractor to us. As such, we have created this specific and detailed Personal Information Privacy Policy (hereinafter referred to as “**this Policy**”) for you to read and appreciate exactly how we safeguard your personal information and respect your privacy when you are a cherished data subject of the organisation.

- Please note that SAMRC is a statutory body parastatal operating in accordance with the laws of South Africa.
- For more information regarding your personal information lawfully stored or used by SAMRC, please contact one of our deputy information officers, who will gladly assist.
- This Policy was last updated on **[21 February 2022]**.
- Not all terms referred to herein are necessarily defined in order.
- Please ensure that you read all the provisions below and our other SAMRC rules and policies, which may apply from time to time and are made available to you, to understand all of your, and our, rights and duties.
- **Notwithstanding a minor’s age, all minors’ parents/guardians will be liable for expressly understanding and agreeing to this Policy and the way SAMRC processes their personal information and the personal information of their child/ward engaging with SAMRC. Accordingly, whilst this Policy is to be expressly understood and accepted by parents only (as it will be binding on them in both a personal and representative capacity), minors may make use of this Policy to understand the processing of their personal information too.**
- Please use the following links to jump to the relevant sections described in this Policy:
 1. ***Important information and who we are***
 2. ***The data we collect about you***
 3. ***How is your personal data collected***
 4. ***How we use your personal data***
 5. ***Disclosures of your personal data***
 6. ***International transfers***
 7. ***Data security***
 8. ***Data retention***
 9. ***Your legal rights***
 10. ***Glossary***

1. Important information and who we are

1.1. Purpose of this Policy

- 1.1.1. This Policy aims to give you information on how SAMRC collects and processes your personal data through any form of your engagement with SAMRC.
- 1.1.2. This Policy complies with and facilitates the obligations required from, the South African *Protection of Personal Information Act, No. 4 of 2013* (“**POPIA**”), as amended.
 - 1.1.2.1. Users with citizenships from jurisdictions other than South Africa, please note that SAMRC complies with all South African data protection laws when processing your personal information pursuant to the Services as we are a South African parastatal operating in South Africa. Should foreign law be applicable in any regard to how we may process your personal information, please contact SAMRC at one of our deputy information offices who will gladly engage you on its application and your rights.
- 1.1.3. It is important that you read this Policy together with any other privacy policy or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you/your child so that you are fully aware of how and why we are using your data. This Policy supplements the other notices and is not intended to override them.
- 1.1.4. **By virtue of the fact that we are a medical and academic science council and parastatal institution and need very particular, and often sensitive information about some of our data subjects to operate and fulfil our mandate, we do process special categories of personal information about our data subjects as well as process the data of minors which all data subjects expressly understand and agree as being absolutely necessary and essential to our operational requirements. Without this information, we simply cannot operate and satisfy our legislated duties. That being said, we do everything in our power to secure and minimise this processing as much as possible, and we proudly explain how we do so herein.**

2. Role as “Responsible Party” and/or “Operator”

- 2.1. SAMRC is the “Responsible Party” (as defined in POPIA) and is responsible for your personal data in instances where we decide the processing operations concerning your personal data.
- 2.2. We also operate as an “Operator” of personal data on behalf of a third-party Responsible Party (such as other governmental authorities/regulators), where that Responsible Party’s privacy terms will apply. Please consult the privacy policy of any such parties to whom you may be providing your personal data as their terms will apply as they are the Responsible Party directing us to process your personal data for their purposes.
- 2.3. We have appointed a Deputy Information Officer (“DIO”) at SAMRC who is responsible for overseeing questions in relation to this Policy. If you have any

questions about this Policy, including any requests to exercise your legal rights, please contact the DIO.

2.4. You have the right to make a complaint at any time to the South African regulator's office (the Information Regulator's Office of South Africa). We would, however, appreciate the chance to deal with your concerns before you approach any such regulator, so please contact us in the first instance.

3. **Changes to this Policy and your Duty to Inform us of Changes**

3.1. This Policy version was last updated on **[21 February 2022]**, and historic versions are archived and can be obtained by contacting us.

3.2. It is important that the personal data we hold about you is accurate and current at all times. This is to ensure the safety and integrity of the valuable information we hold about you. Please let us keep your personal information updated by contacting us should any of your personal information change. We will not know if your personal information changes without you telling us, so please let us know immediately should a change occur. **SAMRC will not be liable for any incorrect personal data it may hold on/about you if you do not notify us of the changes needed.**

4. **Third-Party Links on Website or otherwise**

4.1. The SAMRC Website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements or terms. When you leave our Website or engage with such third parties, we encourage you to read the distinct privacy policy of every third party you engage with.

5. **The data we collect about you and through what avenue:**

5.1. "**Personal data**", or "**personal identifiable information**", means any information about an individual, both natural and juristic entities, from which that entity can be identified. It does not include data where the identity has been removed (anonymous data).

5.2. We may collect, use, store, and transfer ("**process**") different kinds of personal data about you which we have grouped together as follows:

Board Members:

5.2.1. **Identity Data** including full legal names, date of birth, nationality, gender, ethnicity, and proof of ID such as drivers licence, identity card, passport;

5.2.2. **Contact Data** including contact numbers;

5.2.3. **Communications Data** including your preferences in receiving notices.

5.2.4. **Financial Data** including banking details and South African Revenue Services reference numbers/tax directives.

Customer/Clients:

5.2.5. Names, surnames, financial information, banking account details, business addresses;

- 5.2.6. Stakeholder databases, including media houses, universities, Research Offices, Extramural Units, Science Councils, technology transfer offices, government, Vice-Chancellors, Deputy Vice-Chancellors, Research Chairs, healthcare service providers, include the name/surname and contact details of contacts or their representatives.

Contractors who provide us with their services:

- 5.2.7. **Identity/Company Data** including full legal/company names, website details and registration information, CVs of persons employed by the contractors;
- 5.2.8. **Contact Data including** email address, physical address and contact numbers of not just the company but also of employees therein who assist with accounting;
- 5.2.9. **Financial Data** including banking details, VAT number, vendor number, purchase order information, job numbers and SARS reference numbers.

People who use the Website and send us information via it:

- 5.2.10. **Technical Data**
IP addresses.

People who message/telephone us:

- 5.2.11. **Contact Data**
Phone numbers on the telephone management system.

Current employees or prospective hires:

Information captured on Human Resources Information System:

- 5.2.12. - Employee Number
- 5.2.13. - Title
- 5.2.14. - Names
- 5.2.15. - Surname
- 5.2.16. - Dates of Birth
- 5.2.17. - ID Numbers
- 5.2.18. - Citizenship / Nationality
- 5.2.19. - Race
- 5.2.20. - Gender
- 5.2.21. - Marital Status
- 5.2.22. - Disabled Type
- 5.2.23. - Language
- 5.2.24. - Contact Details: Home, Cell number
- 5.2.25. - SAMRC email addresses
- 5.2.26. - Emergency Contact Name and Contact Number

- 5.2.27. - Physical home address
- 5.2.28. - If Foreign National: all the above is captured as well as passport information, work permit.
- 5.2.29. Verification of qualifications, security, and employment checks.

People who walk into our offices for an engagement:

- 5.2.30. **Identity Data** including full legal names/company names;
- 5.2.31. **Vehicle Registration details;**
- 5.2.32. **Video recordings;**
- 5.2.33. **Body Temperature;**
- 5.2.34. **Contact Data** including contact numbers (direct and alternative).

In addition to the above our Research Units process the following data:

- 5.2.35. GPS coordinates of homes, workplace, family members;
 - 5.2.36. Special personal information of various types provided by the data subject in response to questions in a questionnaire, interview, or other data elicitation process;
 - 5.2.37. Biometric records including fingerprints;
 - 5.2.38. Biological samples;
 - 5.2.39. Consent forms;. Information regarding referral e.g., for further medical treatment following an adverse event.
- 5.3. We also collect, use, and share **aggregated/anonymised Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Technical Data to calculate the percentage of users accessing a specific Website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Policy.
- 5.4. Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with our Services).

6. **How is your personal data collected?**

- 6.1. We use different methods to collect data from and about you (such as described above), including through:
 - 6.1.1. **Direct interactions:** Apart from the instances and avenues listed above, we may also collect personal data directly from you when you:
 - 6.1.1.1. complete our forms;
 - 6.1.1.2. are a registered practitioner/member of ours;
 - 6.1.1.3. use our other services as available;
 - 6.1.1.4. request information to be sent to you;

- 6.1.1.5. attend any SAMRC event, whether online or in-person; or
- 6.1.1.6. give us some feedback.

7. How we use your personal data

7.1. We will only use your personal data when the law allows us to and for legitimate reasons, which you hereby expressly understand and consent to. Most commonly, we will use your personal data in the following circumstances:

- 7.1.1. where we have your express consent to do so;
- 7.1.2. where we need to consult with you or perform on the services contract we are about to enter into or have entered into with you;
- 7.1.3. where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests; and/or
- 7.1.4. where we need to comply with a legal or regulatory obligation under law or authority with a lawful mandate/allowance to such information.

8. Purposes for which we will use your personal data:

8.1. We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are, where appropriate, and which exact external third parties your personal data is handed to for the same reasons.

8.2. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

8.3. Due to the fact that we have an extensive network of authorised or statutorily mandated third parties to whom we provide data subjects' personal data, all such third parties cannot be listed in the table below. Should a user want to know exactly which third parties to whom we send your personal data, please contact our deputy information officer who will gladly provide you with the exact requested list.

PURPOSE / ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING INCLUDING BASIS OF LEGITIMATE INTEREST	SPECIFIC EXTERNAL THIRD PARTY TO WHOM THE INFORMATION IS PROVIDED, AND FOR WHAT REASON (IF ANY)
To engage with you after you have contacted us requesting an engagement via the	(a) Identity (b) Contact (c) Technical	(a) Express consent (b) Performance of a contract with you (c) Necessary for our	Not applicable.

PURPOSE / ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING INCLUDING BASIS OF LEGITIMATE INTEREST	SPECIFIC EXTERNAL THIRD PARTY TO WHOM THE INFORMATION IS PROVIDED, AND FOR WHAT REASON (IF ANY)
Website or otherwise		legitimate interests (to keep our records updated and to study how engagees use our services, as well as to develop our services and grow our organisation)	
To provide you with our services as a mandated statutory body (as a member, client or otherwise)	<ul style="list-style-type: none"> (a) Identity (b) Contact (c) Medical (d) Financial (e) Parental / Guardianship (f) Technical (g) Social Media (h) Marketing and Communications 	<ul style="list-style-type: none"> (a) Performance of a contract with you (b) Express consent (c) Necessary to comply with a legal obligation (d) Necessary for our legitimate interests (to provide you with the Services you contracted to acquire from us, and to keep our records updated and to study how engagees use our services) 	Please contact SAMRC at any time to obtain an exact list of such parties.
To provide it to our authorised third-party service providers who need your personal data to provide their private services to you (such as payment service providers, government departments or affiliates)	<ul style="list-style-type: none"> (a) Identity (b) Contact (c) Medical (d) Parental / Guardianship (e) Technical 	<ul style="list-style-type: none"> (a) Performance of a contract with you (b) Necessary for our legitimate interests (to provide you with the Services you have contracted from the authorised third-party, and to develop our services and grow our organisation) (c) Express consent 	Please contact SAMRC at any time to obtain an exact list of such parties.
To process and	(a) Identity	(a) Performance of a	Please contact SAMRC

PURPOSE / ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING INCLUDING BASIS OF LEGITIMATE INTEREST	SPECIFIC EXTERNAL THIRD PARTY TO WHOM THE INFORMATION IS PROVIDED, AND FOR WHAT REASON (IF ANY)
<p>service your payment for any services rendered by SAMRC or its service providers.</p> <p>To manage payments, fees, and charges</p>	<p>(b) Contact</p> <p>(c) Financial</p>	<p>contract with you</p> <p>(b) Necessary for our legitimate interests (to make or receive necessary organisation payments)</p> <p>(c) Express consent</p>	<p>at any time to obtain an exact list of such parties.</p>
<p>To manage our relationship with you which may include notifying you about changes to our terms or Personal Information Privacy Policy or Services</p>	<p>(a) Identity</p> <p>(b) Contact</p> <p>(c) Marketing and Communications</p>	<p>(a) Performance of a contract with you</p> <p>(b) Necessary to comply with a legal obligation</p> <p>(c) Necessary for our legitimate interests (to keep our records updated and to study how engagees use our Services)</p> <p>(d) Express consent</p>	<p>Please contact SAMRC at any time to obtain an exact list of such parties.</p>
<p>To administer and protect our organisation and our Website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)</p>	<p>(a) Identity</p> <p>(b) Contact</p> <p>(c) Technical</p>	<p>(a) Necessary for our legitimate interests (for running our organisation, provision of administration and IT services, network security, to prevent fraud and in the context of an organisation restructuring exercise)</p> <p>(b) Necessary to comply with a legal obligation</p> <p>(c) Express consent</p>	<p>Please contact SAMRC at any time to obtain an exact list of such parties.</p>
<p>To employ or</p>	<p>(a) Identity</p>	<p>(a) Necessary for our</p>	<p>Please contact SAMRC</p>

PURPOSE / ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING INCLUDING BASIS OF LEGITIMATE INTEREST	SPECIFIC EXTERNAL THIRD PARTY TO WHOM THE INFORMATION IS PROVIDED, AND FOR WHAT REASON (IF ANY)
interview staff or prospective staff members	(b) Contact (c) Technical (d) Marketing and Communications	legitimate interests (for running our organisation, provision of administration and IT services, network security, to prevent fraud) (b) Necessary to comply with a legal obligation (c) Express consent	at any time to obtain an exact list of such parties.
To use data analytics to improve our Website, Services, engagee-relationships, and experiences	(a) Technical (b) Identity	(a) Necessary for our legitimate interests (to define types of engagees for our services, to keep our Website updated and relevant, to develop our organisation and to inform our marketing strategy) (b) Express consent	Please contact SAMRC at any time to obtain an exact list of such parties.
To provide you with direct and user-specific marketing, make suggestions and recommendations to you about events or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Marketing and Communications	(a) Necessary for our legitimate interests (to develop our services and grow our organisation) (b) Express consent	Please contact SAMRC at any time to obtain an exact list of such parties.

8.4. Marketing

8.4.1. You may receive marketing communications from us if you are an existing data subject of ours.

8.5. Change of Purpose

- 8.5.1. We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another lawful reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.
- 8.5.2. If we need to lawfully use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.
- 8.5.3. Please note that we may lawfully process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by the applicable law.

9. Disclosures of your personal data

9.1. We may have to share your personal data with the parties set out below for the purposes set out in the table above.

- 9.1.1. Internal third parties as set out in the glossary;
- 9.1.2. External third parties as set out in the glossary;
- 9.1.3. Specific third parties listed in the table above; and/or
- 9.1.4. Third parties to whom we may choose to sell, transfer, or merge parts of our organisation or our assets. Alternatively, we may seek to acquire other organisations or merge with them. If a change happens to our organisation, then the new owners may use your personal data in the same way as set out in this Policy.

9.2. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions and standards.

10. Express Cookies provision

10.1. The SAMRC website may make use of “cookies” to automatically collect information and data through the standard operation of the Internet servers. “Cookies” are small text files a website can use (and which we may use) to recognise repeat users, facilitate the user’s ongoing access to and use of a website and allow a website to track usage behaviour and compile aggregate data that will allow the Website operator to improve the functionality of the Website and its content, and to display more focused advertising to a user by way of third-party tools.

10.2. The type of information collected by cookies is not used to personally identify you. If you do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows you to deny or accept the cookie feature. Please note that cookies may be necessary to provide you with certain features available on our website, and thus if you disable the cookies on your browser you may not be able to use those features, and your access to our Website will therefore be limited. If you do not disable “cookies”, you are deemed

to consent to our use of any personal information collected using those cookies, subject to the provisions of this Policy and our other policies or terms.

11. International transfers

- 11.1. We may share your personal data within the SAMRC group of organisations and affiliates, and this may involve transferring and processing your data outside of South Africa.
- 11.2. Whenever we transfer your personal data out of either territory, we will ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:
 - 11.2.1. We will always have a contract in place covering the processing of data and service provision between the parties; and
 - 11.2.2. We will only provide your personal data to an entity that processes personal information at standards equal to or better than ours; or
 - 11.2.3. We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the South African Information Regulator's office; or
 - 11.2.4. Where we use certain service providers, we may use specific contracts/clauses approved by the South African Information Regulator's office which give personal data the same protection it has in South Africa.
- 11.3. Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of South Africa.

12. Data security

- 12.1. We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. These measures include the following:

1. Lockable offices.
2. Lockable cabinets.
3. Lockable safes.
4. Access control at the main gate.
5. 24hrs security presence at the main gate.
6. Canine assisted security patrol during the night.
7. Electronic Access control to the office blocks.
8. Electronic Access controls to the sections of buildings.
9. 24hrs camera surveillance of the head office buildings and parameter grounds.
10. Keeping of information in files and the storing of the files away in lockable cabinets located within lockable offices and access-controlled building sections.
11. Both Anti-Virus software is deployed on servers and laptops.
12. We have a solution in place that monitors security related incidents on a

24/7 basis. This enables up to proactivity address any security risks.

13. Firewall penetration tests are performed annually to ensure that we are still maintaining a secure network. This includes detail audits of firewall rules.
14. All laptop drives are encrypted .
15. Security audits are performed on an annual basis by the Auditor General of South Africa.
16. Inactive accounts are automatically disabled. New accounts creations are verified with user application forms.
17. In terms of the user policy all data is required to be saved on the servers.
18. Mobile devices are the property of the staff member. To protect SAMRC email users are required to have a password on the device as well as a password to download email. Passwords change every 42 days.
19. Access to the Data Centres is restricted and only via biometric access.
20. Backups are performed daily and stored offsite. Backups are tested quarterly.
21. When staff leave the SAMRC we receive a notification from its Human Resources department. Accounts are then deprovisioned.
22. Access to all data is via the use of Multi Factor Authentication.
23. Information Security Awareness & Training is done internally from time to time.

- 12.2. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a legitimate need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.
- 12.3. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

13. Data retention

- 13.1. We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.
- 13.2. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data, any other South African applicable law requiring us to retain the data and whether we can achieve those purposes through other means, and the applicable legal requirements.
- 13.3. Details of retention periods for different aspects of your personal data are available from us by contacting us.

- 13.4. In some circumstances you can ask us to delete your data; see below for further information.
- 13.5. In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

14. Your legal rights

- 14.1. Under certain circumstances, you have rights under data protection laws in relation to your personal data where we are the relevant “Responsible Party” over such personal data. Please contact us to find out more about, or manifest, these rights:
 - 14.1.1. request access to your personal data;
 - 14.1.2. request correction of your personal data;
 - 14.1.3. request erasure of your personal data;
 - 14.1.4. object to the processing of your personal data;
 - 14.1.5. request a restriction of processing your personal data;
 - 14.1.6. request transfer of your personal data; and/or
 - 14.1.7. right to withdraw consent.
 - 14.2. You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may decline to comply with your request in these circumstances.
 - 14.3. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.
 - 14.4. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.
 - 14.5. **All data subjects understand and agree that although you may have the right to revoke your consent provided to SAMRC to process your data, SAMRC may still have a lawful ground upon which to continue to process your data and will rely on such lawful ground to continue to do so (such as the need to process your data pursuant to our statutory rights to do so as a parastatal).**
-

15. Glossary

15.1. Lawful Basis

- 15.1.1. **Legitimate Interest** means the interest of our organisation in conducting and managing our organisation to enable us to give you the best service and the most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.
- 15.1.2. **Performance of Contract** means processing your data where it is necessary for the performance of a contract to which you are a party (i.e., to provide you with our Services) or to take steps at your request before entering into such a contract.
- 15.1.3. **Comply with a legal or regulatory obligation** means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to (such as the *SAMRC Act, 1991*).
- 15.1.4. **Express consent** means the confirmed express consent you have provided to our processing of your personal data by actively accepting this Policy.

15.2. Third Parties

- 15.2.1. **Internal Third Parties** means other entities or parties in the SAMRC group acting as joint controllers or operators and who are based in South Africa and provide IT and system administration services and undertake reporting.
- 15.2.2. **External Third Parties** means:
 - 15.2.2.1. Authorised third-party service providers under contract with SAMRC who need your personal information in order to contact and transact with you pursuant to your use of our Services (such as banks, lawyers, government departments);
 - 15.2.2.2. specific third parties who have been identified in the table above;
 - 15.2.2.3. service providers acting as processors based in South Africa who provide IT and system administration services;
 - 15.2.2.4. South African or other national/provincial/local governments and/or their respective authorities pursuant to our adherence with anti-corruption, crime-fighting legislation; and/or
 - 15.2.2.5. Professional advisers acting as sub-operators including lawyers, bankers, auditors, and insurers based in South Africa who provide consultancy, banking, legal, insurance and accounting services as required.

16. Your legal rights

16.1. You have the right to:

- 16.1.1. **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- 16.1.2. **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- 16.1.3. **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no valid reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. **Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be communicated to you, if applicable, at the time of your request (most commonly being other national laws requiring us to continue to process your personal data for a lawful, prescribed reason).**
- 16.1.4. **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- 16.1.5. **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - 16.1.5.1. if you want us to establish the data’s accuracy;
 - 16.1.5.2. where our use of the data is unlawful but you do not want us to erase it;
 - 16.1.5.3. where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - 16.1.5.4. you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- 16.1.6. **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided

consent for us to use or where we used the information to perform on a contract with you.

- 16.1.7. **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain Website access or Services to you. We will advise you if this is the case at the time you withdraw your consent. **Please take note that regardless of your right to withdraw consent under POPIA, other South African legislation applies and may require that we continue to process your data in order to comply with anti-corruption, tax, child-care, medical, crime-fighting and/or other national legislation, which you expressly understand and agree to.**

Category:	Level 1
Risk:	Strategic
Effective Date:	March 2022
Review Date:	March 2023
Policy Owner:	President
Policy Manager / Cognisant Person:	General Counsel
Board Approval:	24 February 2022

Confirmation of Approval



.....
Prof G Gray
President

4 March 2022

.....
Date