THE MANDELA RHODES FOUNDATION

BUILDING EXCEPTIONAL LEADERSHIP IN AFRICA

THE MANDELA RHODES FOUNDATION TRUST

DATA PRIVACY POLICY

Effective 1 July 2021

The Mandela Rhodes Building, 150 St George's Mall, Cape Town, South Africa | PO Box 15897, Vlaeberg, 8018, Cape Town, South Africa
T +27 (21) 424 3346 **E** julia@mrf.org.za **W** www.mandelarhodes.org

1. INTRODUCTION AND PURPOSE

1.1. This policy sets out the data protection principles and procedures pertaining to The Mandela Rhodes Foundation Trust, a trust registered in the Republic of South Africa under Master's Reference Number IT5164/2003, whose registered office is at The Mandela Rhodes Building, 150 St George's Mall, Cape Town (the "**Organisation**") ("**Policy**").

1.2. In particular, this Policy summarises how the Organisation processes personal information belonging to, amongst others, its staff, business contacts, beneficiaries, funders, donors, and suppliers ("**data subjects**").

1.3. The Organisation takes the privacy of personal information very seriously, and is committed to processing personal information in accordance with data protection legislation, including the Protection of Personal Information Act (No. 4 of 2013) ("**POPI**") and, where applicable, the General Data Protection Regulation (EU 2016/679), the retained EU law version of the General Data Protection Regulation (EU) 2016/679) as it forms part of the law of England and Wales, Scotland, and Northern Ireland (together, "**GDPR**"), and any other applicable data protection legislation and/or regulation in force from time to time (collectively, the "**Data Protection Laws**").

1.4. This Policy is made available on the Organisation's website (https://www.mandelarhodes.org/) and is otherwise available, on request, from the Organisation's head office.

2. DEFINITIONS

2.1. In this Policy, the following words mean:

2.1.1. **consent**. Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.1.2. **de-identify**. In relation to personal information of a data subject, to delete any information that:

2.1.2.1. identifies the data subject;

2.1.2.2. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

2.1.2.3. can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ''**de-identified**'' has a corresponding meaning.

2.1.3. **Information Officer**. As contemplated in POPI.

2.1.4. **operator**. 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.

2.1.5. **personal information**. Any information relating to a data subject who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the

physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.

2.1.6. **personal information breach**. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored, or otherwise processed.

2.1.7. **process**. Any operation or set of operations performed on personal information or sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.1.8. **Regulator**. The Information Regulator established in terms of section 39 of POPI.

2.1.9. **responsible party**. 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.

2.1.10. **special personal information**. As contemplated in section 26 of POPI, which includes religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; and/or the criminal behaviour of a data subject to the extent that such information relates to:

2.1.10.1. the alleged commission by a data subject of any offence; or

2.1.10.2. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

2.2. In this Policy:

2.2.1. the words "**include**", "**including**" and "in "**particular**" are by way of example only and shall not limit the generality of any preceding words;

2.2.2. if any provision becomes illegal, invalid or unenforceable, such provision shall be severed, to the extent of its illegality, invalidity or unenforceability, from the balance of this agreement; and

2.2.3. the words "**other**" and "**otherwise**" shall be interpreted as widely as possible and will not be limited by any preceding words.

2.3. This Policy has been drafted using the terminology contemplated in POPI. Where this Policy is interpreted in the context of GDPR, the terms:

2.3.1. "**Information Officer**" shall be read as "**Data Protection Officer**";

2.3.2. "**responsible party** " shall be read as " **data controller**";

2.3.3. "**personal information** " shall be read as " **personal data**";

2.3.4. "**Regulator**" shall be read as "**Supervisory Authority**"; and

2.3.5. "**special personal information**" shall be read as "**special category personal information**", as those terms are defined in GDPR.

3. SCOPE

The procedures and principles set out in this Policy must be followed at all times by the Organisation, its employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators processing personal information on the Organisation's behalf.

4. INFORMATION OFFICER

4.1. the Organisation's Information Officer is:

Ernst Gerber | ernst@mrf.org.za | 021 424 3346

4.2. The Information Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

4.3. The Information Officer is tasked with ensuring that all employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators, comply with this Policy and, where applicable, implement all such practices, processes, controls, and training as is reasonably necessary to ensure such compliance.

4.4. Any questions relating to this Policy or to Data Protection Laws should be referred to the Information Officer. In particular, the Information Officer should always be consulted in the following cases:

4.4.1. if there is any uncertainty relating to the lawful basis on which personal information is to be collected, held, and/or processed;

4.4.2. if consent is being relied upon in order to collect, hold, and/or process personal information;

4.4.3. if there is any uncertainty relating to the retention period for any particular type(s) of personal information;

4.4.4. if any new or amended privacy notices or similar privacy-related documentation are required;

4.4.5. if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of a subject's request/s);

4.4.6. if a personal information breach (whether suspected or actual) has occurred;

4.4.7. if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal information;

4.4.8. if personal information is to be shared with third parties (whether such third parties are acting jointly as responsible parties or operators);

4.4.9. if personal information is to be transferred outside of the country in which it is originally processed and there are questions relating to the legal basis on which to do so;

4.4.10. when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities;

4.4.11. when personal information is to be used for purposes different to those for which it was originally collected;

4.4.12. if any automated processing, including profiling or automated decision-making, is to be carried out; or

4.4.13. if any assistance is required in complying with the law applicable to direct marketing.

5. THE RIGHTS OF DATA SUBJECTS

Data subjects have the right to have their personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of POPI. The Organisation is committed to upholding the rights of data subjects, which rights include:

5.1. the right to be notified;

5.2. the right of access;

5.3. the right to rectification;

5.4. the right to correction, destruction or erasure;

5.5. the right to object to or restrict processing;

5.6. the right to data portability;

5.7. rights with respect to automated decision-making and profiling;

5.8. the right to complain to the Regulator; and

5.9. the right to institute civil proceedings in relation to its personal information.

6. DATA PROTECTION PRINCIPLES

6.1. The Organisation is committed to promoting and upholding the conditions for the lawful processing of personal information as set out in POPI, being:

6.1.1. accountability, as contemplated in section 8;

6.1.2. processing limitation, as contemplated in sections 9 – 12;

6.1.3. purpose specification, as contemplated in sections 13 – 14;

6.1.4. further processing limitation, as contemplated in section 15;

6.1.5. information quality, as contemplated in section 16;

6.1.6. openness, as contemplated in sections 17 – 18;

6.1.7. security safeguards, as contemplated in sections 19 – 22; and

6.1.8. data subject participation, as contemplated in sections 23 – 25, of POPI.

6.2. Accordingly, the Organisation is committed to processing personal information only in a manner that:

6.2.1. is lawful and transparent;

6.2.2. is specified, explicit, and legitimate, and for a particular purpose;

6.2.3. is relevant, and limited to what is necessary in relation to the purposes for which it is processed;

6.2.4. is accurate;

6.2.5. permits identification of data subjects for no longer than is necessary or insofar as permitted by Data Protection Law; and

6.2.6. ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

7. PROCESSING OF PERSONAL INFORMATION

7.1. The Organisation shall only process personal information if at least one of the following apply:

7.1.1. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

7.1.2. processing complies with an obligation imposed by law on the responsible party;

7.1.3. processing protects a legitimate interest of the data subject;

7.1.4. processing is necessary for the proper performance of a public law duty by a public body; and/or

7.1.5. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

7.2. No person must share any personal information with the Organization unless they have the requisite consent from the relevant data subject to do so. Where a person transmits any personal information to the Organisation which belongs to a third party, that person warrants that they have obtained the requisite consent for the

Organisation to process such information, and is responsible for notifying the Organisation immediately if such consent is withdrawn.

8. PROCESSING OF SPECIAL PERSONAL INFORMATION

The Organisation shall only process special personal information in accordance with the provisions of Part B of POPI. The processing of special personal information shall be lawful if at least one of the following applies:

8.1. processing is carried out with the consent of a data subject;

8.2. processing is necessary for the establishment, exercise or defence of a right or obligation in law;

8.3. processing is necessary to comply with an obligation of international public law;

8.4. processing is for historical, statistical or research purposes to the extent that:

8.4.1. the purpose serves a public interest and the processing is necessary for the purpose concerned; or

8.4.2. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

8.5. information has deliberately been made public by the data subject; or

8.6. where applicable, the provisions of sections 28 to 33 of POPI, as the case may be, are complied with.

9. SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

The Organisation only collects, processes, and holds personal information where there is a specified, explicit and legitimate purpose.

10. ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING

10.1. The Organisation will only collect and process personal information for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

10.2. Examples of some of the personal information that the Organisation processes include:

10.2.1. Employees / Prospective Employees:
- Name
- Contact details (including email address and contact number)
- Physical address
- Identity number
- Income tax number

10.2.2. Suppliers/Contractors:

•Name
•Contact details (including email address and contact number)
•VAT number
•Bank details (for payments)

10.2.3. Funders
•Name
•Contact details (including email address and contact number)

10.2.4. Beneficiaries/Project Participants:
•Name
•Contact details (including email address and contact number)
•Identity number
•Such other information as required for the relevant project, which may include special personal information

10.3. Employees, agents, contractors, or other parties processing personal information on behalf of the Organisation shall:

10.3.1. collect personal information only to the extent required for the performance of their duties, and only in accordance with this Policy; and

10.3.2. process personal information only when the performance of their duties requires it.

11. ACCURACY OF PERSONAL INFORMATION

11.1. The Organisation shall ensure that all personal information collected, processed, and held by it is kept accurate and up to date.

11.2. If any personal information is found to be inaccurate or out-of-date, all reasonable steps will be taken by the Organisation without delay to amend or erase that data, as appropriate.

12. STORAGE AND RETENTION

12.1. Personal data, is stored by the Organisation in the following ways and in the following locations:

12.1.1. the Organisation's own servers, located in South Africa;

12.1.2. third-party servers, operated by, amongst others:

12.1.2.1. Dropbox, located in the United States and, in certain instances, in Australia, Germany, Japan and the United Kingdom;

12.1.2.2. Mailchimp, located in the United States;

12.1.2.3. Absolute Cloud Solutions located in South Africa;

12.1.2.4. WhatsApp, located in the United States and in certain instances globally;

12.1.2.5. Microsoft SharePoint, located in the European Union;

12.1.2.6. Google OneDrive, located in the United States;

12.1.2.7. Salesforce located in the United States, Germany, Japan, the United Kingdom and France;

12.1.3. computers permanently located at the Organisation's business premises;

12.1.4. laptop computers and other mobile devices provided by the Organisation to its employees, agents, and contractors;

12.1.5. computers and mobile devices owned by employees, agents, and contractors; and

12.1.6. physical records stored at the Organisation's premises, or the premises of the Organisation's partners/affiliates.

12.2. The Organisation shall not keep personal information for any longer than is necessary considering the purpose for which that personal information was originally collected, held, and processed.

12.3. When personal information is no longer required, it will either be de-identified, or all reasonable steps will be taken to erase or otherwise dispose of it without delay.

13. SECURE PROCESSING

13.1. The Organisation shall ensure that all personal information collected, held, and processed by it is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

13.2. All technical and organisational measures taken to protect personal information shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal information.

13.3. The Organisation will adhere to the following guidelines to protect against the confidentiality, integrity, and availability of all personal information:

13.3.1. only those with a genuine need to access and use personal information and who are authorised to do so may access and use it;

13.3.2. personal information must be accurate and suitable for the purpose for which it is collected, held, and processed; and

13.3.3. authorised users must always be able to access the personal information as required for the authorised purpose or purposes.

14. ACCOUNTABILITY AND RECORD-KEEPING

14.1. A data protection impact assessment shall be conducted if any processing of personal information presents a significant risk to the rights and freedoms of data subjects.
14.2. The Organisation's data protection compliance shall be regularly reviewed and evaluated by the Information Officer.

14.3. The Organisation will keep adequate internal records in respect of the processing of personal information.

15. DATA SUBJECT ACCESS

15.1. Data subjects may, at any time, request the Information Officer to supply details as to the personal information which the Organisation holds about that data subject, what the Organisation is doing with that personal information, and why.

15.2. The Organisation does not charge a fee for the handling of normal requests. However, the Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. RECTIFICATION OF PERSONAL INFORMATION

16.1. Data subjects have the right to require the Organisation to rectify any of their personal information that is inaccurate or incomplete. The Organisation shall comply with such requests timeously.

16.2. In the event that any affected personal information has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal information.

17. ERASURE OF PERSONAL INFORMATION

17.1. Data subjects have the right to request that the Organisation erases the personal information it holds about them in certain circumstances, for example, where the data subject withdraws its consent for the processing of its personal information.

17.2. Unless the Organisation has reasonable grounds to refuse to erase personal information, all requests for erasure shall be complied with timeously, and the data subject informed of the erasure.

17.3. In the event that any personal information that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

18. RESTRICTION OF PERSONAL INFORMATION PROCESSING

18.1. A data subject may request that the Organisation ceases processing the personal information it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal information concerning that data subject (if any) that is

necessary to ensure that the personal information in question is not processed further.

18.2. In the event that any affected personal information has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

19. DATA PORTABILITY

Data subjects have the right to receive a copy of their personal information in the Organisation's possession in a structured, commonly used and machine-readable format, and to request its transmission to another entity.

20. OBJECTIONS TO PROCESSING PERSONAL INFORMATION

20.1. Data subjects have the right to object to the Organisation processing their personal information based on legitimate interests, for direct marketing (including profiling), and processing for research and statistics purposes.

20.2. Where a data subject objects to the Organisation processing their personal information based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3. Where a data subject objects to the Organisation processing their personal information for direct marketing purposes, the Organisation shall cease such processing promptly.

20.4. Where a data subject objects to the Organisation processing their personal information for research and statistics purposes, the data subject must demonstrate grounds relating to his or her particular situation. The Organisation is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21. DIRECT MARKETING

21.1. The Organisation shall obtain a data subject's prior consent for direct marketing (including email and text messaging), and shall not approach a data subject more than once for the purpose of obtaining their consent to direct marketing.

21.2. If a data subject objects to direct marketing, the Organisation shall comply with the request promptly.

21.3. The Organisation will not approach a data subject for purposes of direct marketing if that data subject has previously withheld consent.

22. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

22.1. Where possible, the following technical and organisational measures shall be implemented to protect the security of personal information:

22.1.1. appropriate firewalls anti-virus protections shall be implemented and regular malware scans shall be conducted;

22.1.2. emails containing personal information must be marked “confidential”;

22.1.3. personal information should only be transmitted over secure networks;

22.1.4. personal information shall not be transmitted over a wireless network if there is a reasonable wired alternative;
22.1.5. all personal information transferred physically should transferred in a suitable container and marked “confidential”;

22.1.6. all hardcopies of personal information, along with any electronic copies stored on physical media shall be stored securely and appropriate access control measures shall be implemented;

22.1.7. no personal information shall be shared informally, and if access is required in respect of any personal information, such access should be requested in writing;

22.1.8. no personal information shall be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Organisation or not, without prior authorisation;

22.1.9. personal information shall be handled with care at all times and should not be left unattended;

22.1.10. all electronic copies of personal information shall be stored securely using passwords and where appropriate, encrypted;

22.1.11. all passwords used to protect personal information shall be changed regularly;

22.1.12. no passwords shall be written down or shared. If a password is forgotten, it must be reset using the applicable method; and

22.1.13. no unauthorised software may be installed on any computer or device owned by the Organisation, without prior written approval from the Information Officer.

22.1.14. all employees and other parties working on behalf of the Organisation shall be bound to comply with the Data Protection Laws and this Policy;

22.1.15. all employees and other parties handling personal information on behalf of the Organisation shall exercise care and caution when discussing any work relating to personal information;

22.1.16. the methods of collecting, holding, and processing personal information shall be regularly evaluated and reviewed by the Information Officer; and

22.1.17. all agents, contractors, or other parties handling personal information on behalf of the Organisation shall ensure that all persons who have access to such personal information are held to the same degree of care as contemplated in this Policy.

22.2. Where any agent, contractor or other party handling personal information on behalf of the Organisation fails in their obligations under the Data Protection Laws and/or this Policy, that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. TRANSFERRING PERSONAL DATA TO ACROSS BORDERS

The Organisation may, from time to time, transfer personal information to countries outside of the country in which the personal information was collected, but only where one of the following principles applies:

23.1. the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:

23.1.1. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

23.1.2. includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

23.2. the data subject consents to the transfer;

23.3. the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

23.4. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

23.5. the transfer is for the benefit of the data subject, and:

23.5.1. it is not reasonably practicable to obtain the consent of the data subject to that transfer;

23.5.2. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

24. PERSONAL INFORMATION BREACH NOTIFICATION

24.1. All personal information breaches must be reported immediately to the Organisation's Information Officer.

24.2. If an employee, agent, contractor, or other party working on behalf of the Organisation becomes aware of or suspects that a personal information breach has occurred, they shall notify the Information Officer immediately, and shall not attempt to investigate it themselves. All evidence relating to the personal information breach in question should be carefully retained.

24.3. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Organisation shall, as soon as reasonably possible, notify, in writing:

24.3.1. the Regulator (within 72 hours, where GDPR is applicable); and

24.3.2. the data subject, unless the identity of such data subject cannot be established.

24.4. The notification referred to in clause 25.3 shall include, at a minimum, the following information:

24.4.1. a description of the possible consequences of the security compromise;

24.4.2. a description of the measures that the responsible party intends to take or has taken to address the security compromise;
24.4.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

24.4.4. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

24.5. The Organisation may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.