DATA PROTECTION POLICY

of

SOUTH AFRICAN ORTHOPAEDIC ASSOCIATION

(an association within the South African Medical Association NPC, which is an association incorporated under section 23 of the Companies Act, 1973, with registration number 05/00136/08)

(hereinafter referred to as "**the Association**")

ANDERSEN

TABLE OF CONTENTS

1. **OBJECTIVE**

This policy seeks to align best practice in the Association with legal standards governing its members and personnel, including the Protection of Personal Information Act, 4 of 2013.

It is acknowledged that the Association may collect or store Personal Information from its members and process data and Personal Information from its members, in a lawful manner, to enable the Association to provide services that are in line with the Association's legitimate objectives. In addition, the Association collects, processes and stores Personal Information from its own employees for various legitimate purposes, including those related to employment, administration and human resources.

2. **SCOPE**

2.1 Application

2.1.1 This policy applies to all employees of the Association in respect of all Personal Information accessed in the provision of services by the Association to its members, as well as the management of its employment relationships with its own employees.

2.1.2 It applies to all Personal Information that it holds relating to identifiable Data Subjects, including, but not limited to, the following –

2.1.2.1 names of Data Subjects;

2.1.2.2 physical and postal addresses;

2.1.2.3 email addresses;

2.1.2.4 telephone and cell phone numbers;

2.1.2.5 all Personal Information received relating to a Data Subject that is received from a member in the course of providing services; and/or

2.1.2.6 all Personal Information of a Data Subject protected for the benefit of such Data Subject in terms of POPIA.

3. DEFINITIONS

3.1 **"Data Subject"** means any identifiable, living natural person, or identifiable existing juristic person to whom any Personal Information relates;

3.2 **"Information Officer"** means the information officer of the Association, contemplated in terms of section 55 of POPIA, and includes any deputy information officer appointed in terms of section 56 of POPIA;

3.3 **'Personal Information'** means any information relating to a directly or indirectly identified or identifiable natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

3.3.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

3.3.2 information relating to the education or the medical, financial, criminal or employment history of the person;

3.3.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

3.3.4 the biometric information of the person;

3.3.5 the personal opinions, views or preferences of the person;

3.3.6 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;

3.3.7 the views or opinions of another individual about the person; and

3.3.8 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;

3.4 **'POPIA'** means the Protection of Personal Information Act, 4 of 2013, as amended;

3.5 **'Processing'** or '**Processed**' means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, receipt, recording, organisation, collation, structuring, storage, updating, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

4. PROTECTION

4.1 This policy seeks to protect the Association from various real data security risks including breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to the Association and its members, third party data acquired from such members and all its own employees.

4.2 The rules and standards set out in this policy apply regardless of –

4.2.1 whether Personal Information relates to a member or an employee of the Association; and/or

4.2.2 is stored electronically, digitally, on paper, or on other materials, or through other methods.

5. GENERAL RULES RELATING TO PERSONAL DATA

Personal information shall at all times be:

5.1 processed fairly and lawfully, in accordance with POPIA and all other legal standards applicable to such personal information;

5.2 obtained only for specific lawful purposes;

5.3 adequate, relevant and not excessive;

5.4 held for no longer than is necessary for the purpose for which it was obtained;

5.5 processed in accordance with the rights of data subjects as set out in POPIA;

5.6 be protected in appropriate ways, methodologies and procedures, and according to suitable methods, both from an organisation and technology standpoint; and

5.7 not be disclosed or transferred or exported illegally, or in breach of any agreement with a Data Subject.

6. RESPONSIBLE PARTIES

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of Personal Information in the execution of their employment duties to the Association, or

otherwise in the course of rendering services or being associated with the Association.

7. INFORMATION OFFICER

The Information Officer shall –

7.1 be registered as such with the Information Regulator;

7.2 execute, and bear responsibility for reporting to senior management about compliance with POPIA, all technological and operational data protection standards and protocols, and advise of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from such risk or breach;

7.3 ensure that all operational and technological protection of personal information standards are complied with;

7.4 arrange POPIA training and provide advice and guidance in relation thereto to all employees;

7.5 be entitled to suggest to management that disciplinary action be taken against any employee who at any time breaches any technological, organisational and operational data protection standard, rule, instruction, policy, practice and/or protocol of the Association;

7.6 review and approve contracts or agreements with third parties to the extent that such third parties may collect, process and/or store Personal Information; and

7.7 attend to requests from Data Subjects wishing to access and assess Personal Information that the Association retains in relation to them.

8. IT MANAGER

The IT manager of the Association shall –

8.1 ensure that all systems, services and equipment used for processing, and/or storing personal information adhere to POPIA, and internationally acceptable standards of data security and data safeguarding, and that same are updated regularly to continue to comply with such standards;

8.2 issue appropriate and clear guidelines, whether for the Association as a whole or a particular part of it, department, person or level of person in regard to, inter alia, any aspect of the Association's objectives, password protocols, data access protocols, sign-in and sign-off procedures, descriptions of accessories, applications and equipment that will or may be used and/or that may not be used.

9. GENERAL PROTECTION OF PERSONAL INFORMATION RULES

9.1 All Personal Information shall be deemed confidential, and shall be handled as such in terms of POPIA.

9.2 Only persons who require access to Personal Information for the execution of their duties at the Association shall be entitled to access any data covered by this policy.

9.3 Under no circumstances will Personal Information be shared outside the scope of required work outputs or informally. For the avoidance of doubt, an employee shall be entitled to access Personal Information only after obtaining authorisation from the Information Officer or senior management, where any work output requiring access is unusual or out of the ordinary.

9.4 Employees shall keep all Personal Information secure by taking sensible and practical precautions and complying with all rules, practices and protocols.

10. DATA STORAGE

10.1 Paper

10.1.1 Where Personal Information is stored on paper, it shall always be kept in a secure place which prevents unauthorised access. This also applies to Personal Information stored electronically which has been printed out for whatever reason.

10.1.2 When not required, paper containing Personal Information shall be kept in a locked draw, safe or cabinet.

10.1.3 Employees shall ensure that paper and print outs are not left in places that may be open to unauthorised access. This includes, but is not

limited to, in printing trays, in public spaces and in general waste bins. All paper containing Personal Information that is no longer needed, must be shredded immediately.

10.2 **Electronic Data**

10.2.1 Where Personal Information is stored electronically, it shall be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts.

10.2.2 Personal Information shall be protected by strong passwords that are changed regularly and never shared between employees, in accordance with the Association's password policy.

10.2.3 Where Personal Information is stored on removable media such as a USB flash drive, CD or a DVD, these shall at all times be locked away securely when not in immediate use.

10.2.4 All Personal Information shall only be stored on designated drives and servers and shall only be uploaded to cloud computing services approved by the Association.

10.2.5 All servers containing Personal Information shall be located in secure protected locations away from general office space;

10.2.6 Personal Information shall be backed up frequently in accordance with backup protocols set by the IT manager. Such backups shall be tested

regularly in line with the Association's standard backup procedures and protocols under the direction of the IT Manager. The Information Officer (or risk and compliance manager, if applicable) shall be responsible to schedule a minimum of two random tests each year.

10.2.7 No Personal Information shall be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks without prior approval from management.

10.2.8 All servers and computers containing Personal Information will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.

11. DATA USE

11.1 It is acknowledged that Personal Information is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. Therefore, when working with Personal Information, employees shall ensure that screens of their computers are always locked when left unattended.

11.2 Personal Information shall not be shared informally, and in particular it shall never be sent by email without consent of the Data Subject or without protection with appropriate passwords, where required to be sent by email.

11.3 Personal Information shall be encrypted before being transferred electronically. The IT manager, together with the Information Officer, shall

develop and maintain protocols for data transfer to ensure that it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties.

11.4 Personal Information shall never be transferred or sent to any entity that is not directly authorised to receive it.

11.5 Employees are prohibited from saving copies of Personal Information to their own computers and/or devices.

11.6 Employees shall at all times access and update only the central, official copy of any data or work output document, such as payroll.

12. DATA ACCURACY

12.1 Employees shall take all steps legally required by the Association to comply with the Association's rules and work practices to ensure Data is kept accurate and up-to-date.

12.2 The more important the accuracy of any component of Personal Information is, the greater the effort and measures shall be to ensure its accuracy.

12.3 Personal Information must always be held in no more places than is necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional copies.

12.4 Employees shall make use of every opportunity to ensure that any Personal Information is accurate and up-to-date, e.g. by confirming details when handling a call.

12.5 Employees shall, with the assistance of the Information Officer, at all times remain knowledgeable and informed about all data updating practices and work protocols used by the Association, such as updating via official, acknowledged websites and platforms used by members.

13. PROVIDING INFORMATION

In terms of POPIA, Personal Information may be disclosed to law enforcement or other agencies without the consent of the Data Subject. In such circumstance, the Association may be obliged to disclose the requested Personal Information, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Information Officer shall be authorised to furnish the requested Personal Information to the enquiring party.

14. DISCIPLINARY MEASURES

14.1 This data protection policy governs every employee of the Association, both during the course of his/her services to it, and to the extent applicable, after termination of services.

14.2 To the extent that this policy sets out workplace rules governing the employee in the course of his/her work and services to the Association, it

shall form part of the Association's disciplinary code and procedure and is hereby also incorporated into it.

14.3 A breach of any rule in relation to the protection of Personal Information set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

14.4 The imposition of any disciplinary sanction or dismissal shall not preclude the Association from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the Association in the course of pursuing its objectives.