COMPLIANCE FRAMEWORK IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 AND THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000, AS AMENDED FOR:

EY STUART ATTORNEYS

INCORPORATED

REGISTRATION NUMBER: 1999/022245/21

DATA PRIVACY AND SECURITY POLICY

DECLARATION OF ACCEPTANCE

The Board of Directors hereby accepts and adopts this Data Privacy and Security Policy to be integrated and implemented within the Company and its operational structures or systems which may be amended from time to time.

Signed at ***Pretoria*** *on the* ***18*** *of* ***June 2021.***

E.Y STUART

J NELL

B VAN WYK

INDEX

COMPLIANCE FRAMEWORK AND POLICY IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 OF:

EY STUART ATTORNEYS INCORPORATED

REGISTRATION NUMBER: 1999/022245/21

("the COMPANY")

A. INTRODUCTION:

1. EY STUART ATTORNEYS INCORPORATED is a registered personal liability company.

2. The Company is a law firm of practising attorneys registered with the Legal Practice Council in terms of the Legal Practice Act 28 of 2014.

3. The Company's registered business address is and operates from Suite 202, Waterkloof Gardens, 270 Main Street, Brooklyn Pretoria Gauteng.

4. The purpose of collecting data is in the course and scope of the legal profession and applicable legislation.

5. The Company constitutes a private body and thus has a duty to comply with PAIA.

6. The company is regulated by the Companies Act 71 of 2008 and Legal Practice Act 28 of 2014,

1. Definitions

In this document the following definitions as it reflects in Section 1 of the Protection of Personal Information Act 4 of 2013 *("POPIA")* will be used in this document:

1.1 **'Biometrics'** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition

1.2 **'consent'** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

1.3 **‘control’** means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature (note: Control is also used as a synonym for safeguard or counter measure);

1.4 **‘data controller’** means a mandated individual who decides on the manner and purpose for which personal information is processed;

1.5 **‘data subject'** means the person to whom personal information relates;

1.6 **‘data privacy’** means for purposes of this document the act of securing personal data within an organisation by following good practice security procedures and implementing controls in order to confirm that personal data is secure;

1.7 **‘disclosure’** in general terms personal information is disclosed when it is released to parties outside the organisation;

1.8 **'electronic communication'** in terms of the Electronic Communications Act 36 of 2005 means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

1.9 **'Information Officer'** of, or in relation to, a-

a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or*;*

b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

1.10 ‘**Information Officer (Deputy)**’ – (of a private body) means for purposes of this document a person duly designated in terms of Sec. 56 of the Act in order to assist the Information Officer to perform its duties and responsibilities as set out in Sec. 55(1) of the Act and onto which any necessary duties, responsibilities and powers are conferred in order to execute the performance of the duties and responsibilities described in Sec.55(1) of the Act;

1.11 ‘**guidelines**’ means a description that clarifies what should be done and how, to achieve the objectives set out in policies;

1.12 ‘**information processing facilities’** means any information processing system, service or infrastructure, or the physical locations housing them;

1.13 **‘Information Regulator’** means statutory regulatory body established in terms of sec.39 of the Protection of Personal Information Act;

1.14 ‘**information security’** means preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved;

1.15 ‘**information security event’** means an identified occurrence of a system, service or network that is indicating a possible breach of information security policy prescription, or failure of safeguards, or a previously unknown situation that may be security relevant;

1.16 ‘**information security incident’** means an information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security;

1.17 **‘legal entity’** means for purposes of this document, is applied to any organisation within the same ownership chain as an organisation who processes a data owners’ personal information and may include joint ventures(consolidated or unconsolidated), parent companies or any other organisation contracted by the data owner. All direct legal entities are required to adhere to the data owners’ requirements for data privacy and information security;

1.18 **‘media’** means any method of containment of data and information by way of, i.e. written documentation, CD, DVD, audio, visual recording, computerised filing, etc. – in context also referring to public news reporting entities, i.e. newspapers, radio and television reporters or representatives;

1.19 **'operator'** 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;

1.20 **'person'** means a natural person or a juristic person;

1.21 **'personal information'** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to;

a) 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;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

d) the biometric information of the person;
e) the personal opinions, views or preferences of the person;
f) 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;
g) the views or opinions of another individual about the person; and;
h) 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.

1.22 **'policy'** means overall intention and direction as formally expressed by management- the Board of Directors;

1.23 **'private body'** means:

a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
b) a partnership which carries or has carried on any trade, business or profession; or
c) any former or existing juristic person, but excludes a public body;

1.24 **'processing'** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b) dissemination by means of transmission, distribution or making available in any other form; or
c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

1.25 '**production data'** means data that is used and/or produced during the normal day-to-day operations in the organisation;

1.26 **'record'** means any recorded information.

a) regardless of form or medium, including any of the following:

(i) writing on any material;
(ii) 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;
(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
(iv) book, map, plan, graph or drawing;

(v) photograph, 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;

b) in the possession or under the control of a responsible party;
c) whether or not it was created by a responsible party; and
d) regardless of when it came into existence.

1.27 **'responsible party'** 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.

1.28 **'risk'** means combination of the probability of an event and its consequence;

1.29 **'risk evaluation/ assessment'** means process of comparing the estimated risk against given risk of this document,

1.30 **'sanitation'** for the purposes of this document means the process of removing all traces of a data subject's or owner's personal information from hard drives and other data storage media, before such equipment is exchanged, sold, discarded, passed to a new user or used for non-company purposes;

1.31 **special personal information'** means the personal information listed in section 26 of the POPIA and includes:

(a) 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

(b) the criminal behaviour of a data subject to the extent that such information relates to-

(i) the alleged commission by a data subject of any offence; or
(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

1.32 **'third party/subcontractor/operator'** – any entity, whether an individual or a company, who is not part of a responsible party's organisational structure, but works with the responsible party, or processes personal information of the responsible party under authority of and on the responsible party's behalf;

1.33 **'threat'** means a potential cause of an unwanted incident, which may result in harm to a system or organisation;

1.34 **‘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**.**

1.35 **‘vulnerability’** means a weakness of an asset or group of assets that can be exploited by one or more threats.

2. Duty to comply with the POPIA.

2.1 The Company must keep certain records in terms of the following applicable legislation:

2.1.1 Companies Act 71 of 2008 *(“the Companies Act”);*
2.1.2 Legal Practice Act 28 of 2014;
2.1.3 Financial Intelligence Centre Act 38 of 2001 (as amended) *(“FICA”);*
2.1.4 Disaster Management Act 57 of 2002 (as amended);
2.1.5 National Credit Act 34 of 2005;
2.1.6 Labour Relations Act 66 of 1995; and
2.1.7 Basic Conditions of Employment Act 75 of 1997.

and may receive other information within its course and scope of the legal profession. Information is also gathered during its day-to-day administration and management, which includes personal information and, as such, the Company is a responsible party as defined in the POPIA.

2.2 The Company is committed to comply with the provisions of the POPIA in as far as it relates or pertains to its operations.

2.3 The Company recognises the Constitutional privacy rights of all individuals, subject to any applicable legal requirements regarding the privacy of personal information.

2.4 The Company also recognises the importance of client privacy and the sensitivity of the personal information concerning any individual that may be contained on the Company information storage systems.

2.5 As a practicing legal institution, the Company has a professional and ethical obligation to keep confidential all information received within an attorney-client relationship, subject to the client’s instructions to provide legal services.

2.6 The Company is therefore committed to safeguarding the privacy of all personal information in its possession or under its control concerning any individual as

may be required under all current and applicable legislation and to subscribe to all individual Privacy Rights as will be set out according to this Data Privacy Policy.

2.7 **Details of the information officer:**

The Information Officer in terms of POPIA is:

Full names: **BIANCA IDALINA**

Surname: **VAN WYK**

Identity number: **880224 0192 08 9**

Contact details: **biancav@eyslaw.co.za/ 012 346 2302/ 076 690 9548**

Designation: **DIRECTOR**

The information officer is the person described in the PAIA as the head of the company and who must be appointed in terms of the POPIA.

In the Company, the Chief Information Officer will be designated director as resolved by the Board of Directors from time to time.

Duties of information officers of the Company shall specifically include the following:

i) To make sure that the Company's Data Privacy and Security Policy is updated and readily available for inspection;

ii) To ensure that authorisation is obtained from the Regulator where the Act requires (applicable to processing of unique identifiers for purposes other than the purpose for which it was collected – for instance processing of biometrics used for access control to assist in a criminal investigation);

ii) To ensure that data breaches are reported to the Regulator and the data subject and Security Policy with the Company;

iv) To ensure the implementation, monitoring and enforcement of the Data Privacy

v) To monitor and attend to data subject access requests

2.8 **Details of the deputy information officers:**

The Deputy Information officers of the Company are the following persons:

Full names: **YOLANDI**

Surname: **STRICKER**

Identity number: **790919 0157 08 9**

Contact details: **yolandi@eyslaw.co.za / 012 346 2302/ 078 9402 399**

Designation: **LEGAL SECRETARY**

Full names: **MARGARETHA**

Surname: **REINECKE**

Identity number: **831115 0180 08 4**

Contact details: **marga@eyslaw.co.za / 012 346 2302/ 082 967 6896**

Designation: **LEGAL SECRETARY**

Full names: **JOHANNA JACOMINA MARITA**

Surname: **BESTER**

Identity number: **8306150045089**

Contact details: **collections6@eyslaw.co.za / 012 346 2302/ 071 212 2894**

Designation: **LEGAL SECRETARY**

The Deputy Information Officers may consist of any number of professional or support staff in the employ of the Company alternatively an external third party may be contracted to the Company to assist with management and compliance as assigned by the Information Officer from time to time.

B. THE OUTCOME OF THE PERSONAL INFORMATION IMPACT ASSESSMENT OF THE COMPANY:

1. In terms of regulation 4 of the regulations promulgated under the POPIA, the information officer must cause a personal information impact assessment to be executed on behalf of the company, the purpose of which is to ensure that adequate measures and standards are in place in order to comply with the conditions of the lawful processing of personal information as provided for in the POPIA.

2. As a function of the Company, the following information may be processed in the normal course of the management and administration of the company and law firm:

i. Details of all its employees, which details include but not limited to names, surnames, identity numbers, contact details, biometrics, residential and postal address, bank account details, credit and criminal records, all documentation required in terms of and the Disaster Management Act and all applicable labour legislation;

ii. Details of clients, which includes names, surnames, identity numbers and contact details, biometrics residential and postal address, bank account details, source documents pertaining to the instructions received, and all documentation required in terms of FICA and the Disaster Management Act;

iii. Details of contractors or service providers gaining access to the Company or employed for purposes of rendering services to clients including the personal details of representatives of such service providers and contractors including their names, surnames, identity number and contact details.

3. In exercising its powers and functions, the Company furthermore contracts or may have obligations with third parties or institutions which includes and is not limited to:

3.1 Legal Practitioners – Correspondent Attorneys, Legal Counsel;
3.2 Experts;
3.3 Tracing agents and agents;
3.4 Officers of the Court i.e. Sheriffs, Offices of the Master of the High Court, Courts, Family Advocate;
3.5 Community Schemes Ombud Services;
3.6 Companies and Intellectual Property Commission;
3.7 Deeds office;
3.8 Financial Institutions and Insurance Companies; and
3.9 Service Providers i.e. Network Alliance, RVN Chartered Accountants and Ghost Practice, Office 365.

who may receive access to and process personal information of the aforesaid persons or categories of persons. In this regard, the Company shall do the following:

a) enter into an agreement with third parties where necessary; or
b) request a warranty from such contactors, experts, service providers in substantially the same form as annexure “A” to this framework in order to safeguard the Company and its clients personal information;

c) ensure that only necessary information is disclosed in order to comply with applicable legislation or legal processes.

C. PROTECTION OF PERSONAL INFORMATION

1. Information to be kept and preserved by the Company:

1.1 **In terms of the Companies Act, the Company must process the following information and/or documentation:**

a) Copy of the Memorandum of Incorporation and Shareholders Agreement as well as record of amendments effected;
b) Records of the current directors of the company, including full names, identity number, occupation, date of most recent election or appointment as director and such further information as required in terms of the Act;
c) Records of past directors as described in (a) above for a period of seven years;
d) Copies of reports presented at general meetings of the company for a period of seven years;
e) Notices and minutes of all members' meetings, including resolutions taken by Directors and documents made available to the members in respect of such a resolution – for a period of seven years;
f) Copies of written communication to all shareholders;
g) Minutes and resolutions of every directors' meeting, directors' committees' meeting, audit committee meetings for a period of seven years;
h) And such further information as required in terms of the Act.

1.2 **In terms of the Legal Practice Act, the Company must process the following information and/or documentation:**

a) Names, identity numbers, contact details of Legal Practitioners in the employ of the Company;
b) Names, identity numbers, contact details of Candidate Attorneys registered to complete Articles of Clerkship;
c) Accounting records;
d) Client information to be safely stored for a period of 7(seven) years;
e) And such further information as required in terms of the Act.

1.3 **In terms of the FICA , the Company must process the following information and/or documentation:**

a) Names, identity numbers, residential and postal address, source of income, bank account of details, contact details of clients;
b) All supporting documents for the purpose of identifying and verifying who the client (data subject) is as per items listed in sub-paragraph a);
c) And such further information as required in terms of the Act.

1.4 **In terms of the Disaster Management Act, the Company must process the following information and/or documentation:**

a) Names, identity numbers, residential and postal address, contact details, temperatures;
b) Medical information and certificates;
c) List of symptoms as per National COVID19 guidelines and regulations;
d) And such further information as required in terms of the Act.

1.5 **In terms of the applicable labour legislation, the Company must process the following information and/or documentation:**

a) Names, identity numbers, residential and postal address, contact details, bank account details, credit and criminal records of all employees or employment candidates;
b) Curriculum Vitae with supporting documentation for recruitment**;**
c) Employment contracts;
d) Record of grievances and disciplinary action;
e) Documents pertaining to legal action;
f) And such further information as required in terms of the Act.

Note: At any given time the Company may need to comply with various legislation during the course and scope of its profession.

1.6 **In terms of the day-to-day administration of the Company may process the following personal information:**

Information relating to access control into the Company, including:

a) Names, identity numbers, contact details and designations of visitors and contractors;
b) Data of clients as stipulated above;
c) Data of employees – which may be amended from time to time as stipulated above;
d) Record of manual financial transactions – payments received and made accordingly.

1.7 **Categories of information collected:**

a) Personal details including medical or health information;
b) Financial details, bank statements and supporting documents;
c) demographic information: gender; nationality; salutation; tile
d) language preferences;
e) identifier information: passport or national identity number;
f) contact details: email address, contact number and address;
g) Company documents;
h) Trust documents;
i) Agreements and contracts;
j) supporting documents relating to legal matters wherein we are instructed to act as legal representatives;
k) personal Information included in correspondence, documents, evidence or other materials that we Process in the course of providing legal services;
l) attendance records: details of meetings and other events organised by the Company;
m) consent records;
n) details relating to your visits to our Website and browser settings
o) your employer details;
p) content and advertising data: records of your interactions with our online advertising and content.

2. Purpose of processing information

The Company will process your personal information in the ordinary course and scope of the business, providing legal and related services. The Company and its employees will primarily use your personal information only for the purpose for which it was originally or primarily collected. Personal information will be utilised for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which it was collected.

3. Limitation on information processed and the "minimum information" rule:

The Company must record the minimum possible personal information of employees, visitors and contractors and representatives of contractors in order to comply with its security enforcement obligations, but to simultaneously balance the rights of data subjects.

The Company must furthermore process the minimum amount of personal information of directors and shareholders necessary to comply with the Companies Act and to conduct the day-to-day management and administration of the Company for the benefit of all parties involved.

4. Responsible processing of personal information of clients of the Company:

4.1 The Company and its employees will in the course of its day-to-day business specifically process personal information of its clients, including but not limited to communication with its clients via electronic mail.

4.2 The Company must ensure that clients' personal information, including e-mail addresses, contact details, details pertaining to legal matters, financial and bank account details are protected.

4.3 Care should be taken when communications are sent to clients and appointed third parties as defined in this policy, to ensure that personal information does not land in the hands of unintended recipients. In this regard:

4.3.1 all correspondence and information pertaining to a client and their matter(s) should be sent to the correct person(s);

4.3.2 e-mail addresses of clients should not be visible in general communication to all clients, service providers or third parties (i.e. must be blind carbon copied, or ***Bcc'd***); and

4.3.3 e-mails of persons should not be forwarded to third parties without any permission from the author thereof or without any other lawful reason.

4.3.4 certain documents will be encrypted with a security password that can only be accessed by the appliable client**.**

4.4 The Company shall consider amendment of this policy and guidelines from time-to-time in order to protect personal information of its clients and their legal matters (i.e. steps to be taken in cases of data breaches or in cases where data has been sent to unintended recipients of communication or who obtains access to personal information by bona fide error or other unlawful manner).

4.5 The IT policy clearly outlines the onus on the Company to verify the intended recipients and their relevant contact details. The risk of spam, spoofing, phishing has been disclosed and software known as Mimecast has been installed on all operating systems to divert such threats.

4.6 The Company may be required to disseminate or transfer personal information across borders, outside the Republic of South provided that the country in question has privacy laws in place that will protect the data subject and personal information in a similar fashion to POPIA. This method of disclosure will only be

done so at the explicit request of the client and provided that secured services, correspondence and compatible legal authorities are involved in authenticating the documentation and verifying the identity of the recipient.

5. Storage of personal information and security of information:

5.1 all personal information shall at all times be kept secured by the Company.

5.2 In the case of physical (hard copy documents), such information shall be stored in a lockable cabinet, a safe room or safe, depending on its nature.

5.3 Only authorised persons, which includes the information officer and employees authorised by the information officer, shall have access to such personal information.

5.4 In the case of digital data or data in the cyber space, such data containing personal information shall be stored on a password protected hard drive, Ghost Practice or Convey which is only accessible to registered users, alternatively with a POPIA compliant operator in the cloud, which is only accessible by password which the information officer and authorised personnel has.

6. Information processed which should be destroyed as soon as possible after its purpose was served:

6.1 The Company must securely and effectively dispose of redundant personal information of data subjects on the Company's information systems as soon as possible after the fulfilment of the originally stated purposes, unless prohibited by the requirements of any other applicable legislation.

The Company is under no obligation in law to keep the following personal information for extensive periods:

a) Access control information, including:

ii. Full names and identity information of visitors, contractors or employees; and

iii. Contact details of visitors, contractors or employees.

b) Information including biometric data, contact details and other personal information of visitors and clients entering the Company's premises;

Note: Any of the aforesaid personal information which is not required by law to be kept on record for a fixed period should be destroyed by the responsible

party. In this regard, the Company shall destroy any personal information which is processed for a specific administration purpose (such as security and access control) only for as long as same may serve a purpose and for no longer than 3 (three) months, unless it is necessary to further process the information for a lawful purpose (e.g. to assist the National Command Council with track and trace or any law enforcement authorities with an investigation by authorities regarding a security breach).

6.2 All data must be disposed of securely when no longer required, using formal procedures. The Company must establish formal procedures for the secure disposal of personal information must be established to minimise the risk of confidential information leakage to unauthorised persons.

6.2.1 The procedures for secure disposal of documents containing confidential information must always be proportional to the sensitivity of that information.

6.2.2 The following guidelines must be considered:-

a) media containing confidential information must be stored and disposed of securely, *e.g*. by incineration or shredding, or erasure of data for use by another application within the Company;

b) procedures must be in place to identify the items that might require secure disposal;

c) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

d) many organisations offer collection and disposal services for media - extreme care must always be taken in selecting a suitable external party with adequate controls and experience if and when the function cannot be performed properly internally;

e) disposal of sensitive items must be logged in order to maintain an audit trail.

6.3 The Company shall employ one of the following methods of disposal:

6.3.1 Shredding of paper-based documents;
6.3.2 Deletion of electronic information;
6.3.3 Incineration of paper based documents;
6.3.4 Extraction and return of all personal information to the data subject.

7. Consent to processing of personal information by data subject:

In terms of the POPIA, processing of personal information is allowed once consent of the data subject is obtained.

The processing of personal information must still be for a lawful purpose or for a legitimate objective and may relate to specific personal information.

Attached to this policy is an example of a consent form.

8. Training

a) The Company shall train its employees on a continual basis as necessary, but at least yearly, regarding compliance with the processing of information and destruction of unnecessary information.
b) Operators shall be vetted by the Company (and through its employees or contractors appointed for such purpose, where applicable) to ensure compliance with the POPIA by said operators such as service providers of the community scheme;
c) Training feedback questionaries shall be completed by all participants of the training provided by the Company in order to actively monitor and control the protection of personal information.
d) The Company shall furthermore utilize any training feedback in order to adapt, update and improve this manual every 12 (twelve) months;
e) The Deputy Information Officers will ensure the implementation of the training received.

9. Management and Enforcement

The Company clearly defines what personal information and documents constitutes, communicates and assigns accountability for its privacy policy and procedures to each department within its operational structure. As a Responsible Party it monitors compliance with its Policy. Management has procedures in place to address privacy-related complaints disputes and transgressions.

9.1 The Monitoring system provides for the protection, insertion, amendment and deletion of personal information as elected by the client or service provider from time to time. This is founded on the following management principles:

9.1.1.1 ***Notice***

The Company provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed as per the **Consent Form.**

9.1.1.2 ***Choice and Consent***

The Company describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information as per the **opt-in/opt-out link** attached to all our correspondence, newsletters, notifications and website.

9.1.1.3 ***Collection***

The Company collects personal information only for the purposes identified in the notice and Consent Form.

9.1.1.4 ***Use and Retention***

The Company limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent and retains the information for only as long as necessary to fulfil the stated purposes.

9.1.1.5 ***Access***

The Company provides individuals with convenient access to their personal information for review and updates.

9.1.1.6 Disclosure (*to third parties*)

The Company discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

9.1.1.7 Security (*for privacy*)

The Company protects personal information against unauthorised access (both physical and logical).

9.1.1.8 Quality

The Company maintains accurate, complete and relevant personal information for the purposes identified in the notice.

9.2 The following security measures, tools and processes have been established to ensure compliance:

a) Utilisation of Consent Forms for clients;
b) Implementation of Third Party Confirmation of Compliance form;
c) Opt-in/Opt-out link available on all correspondence;
d) All personal documents or information is stored securely online or within the Company premises or storage lock-up facilities with access restricted to the Board of Directors or employees who require access codes;
f) The premises are secured with an alarm system and security guards;
g) Adherence to the Company IT and Communications policy;
h) Ransomware and Back-up recovery policy;
i) Secure password access to all Company Devices;
j) Restricted password access and user registrations to our online support programs i.e. Ghost Practice, Ghost Convey, Lexis Nexis, E4, Search Works;
k) Regular user updates, deletion of ex-employees and onboarding of new employees;
l) Data Management Software accessible by the appointed Information Officer;
m) All employees are familiar with the Company's confidentiality policy as cited in their employment contracts

10. Breach of Data Security

A breach of data security is defined as "***The actual or potential loss of personal data and/or any information that could lead to identity fraud or have any other significant impacts on individuals or the Company***"

10.1 Identifying breach of data security, which includes, but is not limited to:-

a) Loss or damage to paper-based files containing classified or personal identifiable information;
b) Loss of computer equipment due to crime or an individual's carelessness;
c) Loss of unencrypted computer media e.g. CD, data stick, laptop or other portable devices;
d) Corrupted data;
e) Access to inappropriate websites in breach of policy;
f) Act of Crime- theft, fraud, robbery, forceful entry on the Company premises
g) A computer virus, ransomware, hacking;
h) Accessing a system or computer using someone else's authorisation code, Allowing uncleared and/or un-identified third party IT or other contractor personnel to work on information security systems of the Company;
i) Bona fide error or by accident;
j) Discussing or disclosing personnel or any other data subject's personal information with unauthorised parties;

k) Unsecured handling of information;
l) Any violation of provisions of POPIA and this policy.

10.2 Reporting breach of data security

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 Company Information Officer is obliged under Section 22 (1) of Act to notify the Regulator and also (subject to Section 22 (3) of the Act) the data subject of the event/incident.

In terms of this policy all Company employees and third-party contractors to the Company are obligated to report any breach, or suspected breach of data security immediately to the Company Information Officer or the Board of Directors.

Any employee found to be responsible for an event where a breach of data security occurs through negligence, non-compliance to the Company's policy, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Company.

The contractual agreements of external third-party contractors or operators of the Company will be subject to immediate suspension or termination in the sole discretion of the Board of Directors, pending investigation and recommendations of the Information Officer.

A data breach report will be prepared and furnished to the Board of Directors for consideration within 30 days of the data breach.

In the event of a monetary loss to the Company as a direct result of the occurrence of the breach in Information Security, the accountable party, or parties in both instances may be held fully liable for the loss and any costs for recovery thereof in the sole discretion of the Board of Directors.

11. Risk Assessment and Procedures

The Company is to undergo risk assessment from time to time in order to identify vulnerable areas within the Company structure and possible threats to breach of data privacy.

D. THE PROMOTION OF ACCESS OF INFORMATION ACT 2 OF 2000 (PAIA) AND ACCESS TO INFORMATION IN TERMS OF THE COMPANIES ACT

1. Any person may request information held by the Company in terms of the PAIA. The Board of Directors may, in addition to the PAIA, also request specified records or information in terms of section 26 of the Companies Act.

2. Persons other than the Board of Directors may request copies of the Company's founding documentation and register in terms of section 26 of the Companies Act.

3. Persons other than clients may request information in terms of the PAIA.

4. Requests for access to information in terms of the PAIA is dealt with in the Company's PAIA manual, including:

    a) The format of the request and requirements to be met before information shall be released;
    b) Timelines for processing information pursuant to a request in terms of PAIA as well as the decision to make information available;
    c) The form in which information is to be made available;
    d) Recovery of costs of information processing and dispatch in terms of PAIA;
    e) POPI Act Reference guide.
    f) A quick reference guide on the processing of personal information, the retention and storage thereof as well as the destruction of information is annexed to the policy and **Annexure "B".**

ANNEXURE "A"

GUARANTEE IN RESPECT OF COMPLIANCE
With the Protection of Personal Information Act 4 of 2013 ("POPI Act")

BY: OPERATORS

COMPANY NAME:

("the OPERATOR")

REGISTRATION NUMBER:

AUTHORISED RESPRESENTATIVE:

IN FAVOUR OF:

EY STUART ATTORNEYS INCORPORATED

REGISTRATION NO: 1999/022245/21

("the RESPONSIBLE PARTY")

I, the undersigned _____ in my capacity as _____ duly authorised representative on behalf of _____ ("the Operator") hereby declare that the Operator is POPI Act compliant and that any personal information which is processed in the course of the Operator's functions and services rendered to EY STUART ATTORNEYS INCORPORATED ("the Responsible Party") shall be processed in accordance with the POPI Act.

The Operator hereby indemnifies and holds harmless the Responsible party against any claims by any third party who alleges personal information breaches and/or irresponsible processing of personal information and/or any action or omission which may, if proven, lead to an offence being committed in terms of the POPI Act, where such personal information was not adequately protected in terms of the POPI Act due to an act or omission on the Operator's part.

I further declare that I am the information officer, alternatively the duly appointed agent of the Operator and I am duly authorised on behalf of the Operator to execute this compliance declaration.

I acknowledge and understand that I may incur personal liability in terms of the penalties applicable for committing an offence under the POPI Act should I sign this document without authority of the Operator or if this warrantee is breached.

Dated and signed at _____ on this the _____ day of _____ **2021**

Full names and surname: _____

Identity number: _____

Contact details: _____

Physical Address: _____

_____

_____

_____

obo the Operator who warrants his authority to do so

ANNEXURE "B"

QUICK REFERENCE GUIDE

on the Protection of Personal Information Act 4 of 2013 ("the POPI Act")

1. The POPI Act came into partial operation on the 1st of July 2020 and will become fully operational on 30 June 2021. After this date all responsible parties need to comply with the Act.

2. The purpose of the POPI Act is to promote protection of personal information which information is processed by public and/or private bodies. EY STUART ATTORNEYS INCORPORATED, "the Company" it therefore a private body.

3. The Act prescribes certain requirements for the processing of personal information to ensure that such processing is reasonable, and that personal information is adequately protected.

4. Personal information has a wide meaning, and the Act defines personal information as follows:

4.1 *Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:*

a) 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;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
d) the biometric information of the person;
e) the personal opinions, views or preferences of the person;
f) 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;
g) the views or opinions of another individual about the person; and
h) 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.

4.2 Other definitions which are important to note for purposes of this guide are as follows:

Data-subject:

Is the person to whom personal information relates.

Information officer:

- ***a)*** *public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or;*
- ***b)*** *private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.*

Processing:

Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including

- ***a)*** *the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;*
- ***b)*** *dissemination by means of transmission, distribution or making available in any other form; or*
- ***c)*** *merging, linking, as well as restriction, degradation, erasure or destruction of information;*

Responsible party:

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.

5. Viewed practically, the following basic principles apply when personal information of data-subjects is processed:

    5.1 The minimum amount of information to serve the purpose thereof must be collected;

    5.2 The information must be kept in a safe place to which access is limited to the Information officer or the data collector authorised by the information officer – to avoid intentional and/or unintentional/accidental disclosure to third parties;

    5.3 Personal information which was processed and stored must only be kept for as long as it may be necessary in terms of the purpose for which it was collected and as soon as it does not serve a purpose or is not required to be stored, it must be destroyed.

6. When personal information is processed (i.e. handled, collected etc.), individual data-subjects' information must not be visible to other data-subjects;

7. If personal information is processed, it should be stored in a safe place where third parties do not have access to said personal information;

8. If personal information was stored after processing, it must be destroyed as soon as it has served its purpose, for example:

    8.1 When an entry log is signed to gain access to the property of a private and/or public body, the minimum information must be collected to comply with security protocol, the information must only be stored for a minimum amount of time in order to comply with security protocol (i.e. no more than a month or two, depending on the necessity of record-keeping and the purpose for which the information is collected), the information collected must not be divulged to any other party than the relevant data subject from which it is collected or processed and, finally, the personal information must be destroyed in a manner so that it is not retrievable after destruction (i.e. shredding, deletion or destruction by the private body, alternatively, recycling, destruction or deletion by a responsible third party operator which is POPI Act compliant).

    8.2 Where information of a data-subject is processed and it required to be stored or extensive periods of time in terms of statute, it must be stored in a safe place which is not accessible to third parties and after the prescribed statutory period, it must be destroyed in an irretrievable manner (i.e. shredding, deletion or destruction by the private body, alternatively, recycling, destruction or deletion by a responsible third party operator which is POPI Act compliant).

9. The general rule of thumb when working with personal information of a data-subject is as follows:

    9.1 Only record necessary information to serve the purpose for which it is processed (i.e. scanning of driver's licence and licence disk to gain access to the scheme for security purposes, temperature readings taken for compliance with the Disaster Management Act regulations applicable from time to time);

    9.2 Don't store the information if it will serve no purpose or if it is not prescribed by legislation;

    9.3 Destroy information as soon as possible after it had become redundant (i.e. where it becomes unnecessary to keep or when prescribed periods for record keeping elapses);

    9.4 Never give out any personal information collected to third parties;

    9.5 When in doubt, contact your information officer for directions relating to personal information which you have processed and/or are about to process in the course and scope of your employment or other contract.

MANUAL in terms of section 51 of the Promotion of Access to Information Act 2 0f 2000 ("PAIA") as amended:

In respect of:

EY STUART ATTORNEYS INCORPORATED

REGISTRATION NUMBER: 1999/022245/21

("the COMPANY")

IMPORTANT DEFINITIONS CONTAINED IN THE PAIA

'Head' of, or in relation to, a private body means

(a) in the case of a natural person, including a person referred to in paragraph *(c)* of the definition of 'political party', that natural person or any person duly authorised by that natural person;

(b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;

(c) in the case of a juristic person:

(i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or

(ii) the person who is acting as such or any person duly authorised by such acting person; or

(d) in the case of political party, the leader of the political party or any person duly authorised by that leader;

'official' of, or in relation to, a private body means

(a) any person in the employ (permanently or temporarily and fulltime or parttime) of the public or private body, as the case may be, including the head of the body, in his or her capacity as such; or

(b) a member of the public or private body, in his or her capacity as such.

'Person' means a natural person or a juristic person.

'Personal requester' means a requester seeking access to a record containing personal information about the requester;

'Record' of, or in relation to, a public or private body, means any recorded information

(a) regardless of form or medium;

(b) in the possession or under the control of that public or private body, respectively; and

(c) whether or not it was created by that public or private body, respectively;

'Request for access', in relation to

(a) a public body, means a request for access to a record of a public body in terms of section 11; or

(b) a private body, means a request for access to a record of a private body in terms of section 50;

'Requester', in relation to*:*

a) a public body, means

(i) any person (other than a public body contemplated in paragraph *(a)* or *(b)* (i) of the definition of 'public body', or an official thereof) making a request for access to a record of that public body; or

(ii) a person acting on behalf of the person referred to in subparagraph (i);

(b) a private body, means

(i) any person, including, but not limited to, a public body or an official thereof,

making a request for access to a record of that private body; or

(ii) a person acting on behalf of the person contemplated in subparagraph (i);

INTRODUCTION AND DESCRIPTION OF THE PRIVATE BODY:

1. **EY STUART ATTORNEYS INCORPORATED** is a registered personal liability company.
2. The Company is a law firm of practising attorneys registered with the Legal Practice Council in terms of the Legal Practice Act 28 of 2014.
3. The Company's registered business address is and operates from Suite 202, Waterkloof Gardens, 270 Main Street, Brooklyn Pretoria Gauteng.
4. The purpose of collecting data is in the course and scope of the legal profession and applicable legislation.
5. The Company constitutes a private body and thus has a duty to comply with PAIA.
6. The Company is duly regulated by the Companies Act 71 of 2008 and the Legal Practice Act 28 of 2014.

CONTACT DETAILS OF THE HEAD OF THE COMPANY:

7. The head of the Company shall be deemed to be one of the Directors appointed from time-to-time. In this instance BIANCA IDALINA VAN WYK will be deemed the head of the Company in accordance with this Policy and PAIA.

8. The contact details of the Board of Directors are as follows:

Full names: BIANCA IDALINA
Surname: VAN WYK
Identity number: 880224 0192 08 9
Contact details: biancav@eyslaw.co.za/ 012 346 2302/ 076 690 9548
Designation: DIRECTOR

Full names: ELMO-YORK
Surname: STUART
Identity number: 600229 5033 08 8
Contact details: elmo@eyslaw.co.za/ 012 346 2302/ 082 559 8175
Designation: DIRECTOR

Full names: JO-HANNA
Surname: NELL
Identity number: 740723
Contact details: ona@eyslaw.co.za/ 012 346 2302/ 082 568 2978
Designation: DIRECTOR

9. The Human Rights Commission, in terms of Section 10 of PAIA, issued a guide on how to use the PAIA, which is published in several languages and available at www.sahrc.org.za. The electronic version of the guide is available on request from the managing agent or chairperson of the HOA.

SUBJECTS ON WHICH RECORDS ARE HELD BY THE COMPANY:

10. **The company holds records of information on the following subjects and for the following periods:**

a. In terms of section 24 of the Companies Act, the Company must keep records of following information and/or documentation:

i. Copy of the Memorandum of Incorporation and Shareholders Agreement as well as record of amendments effected.

ii. Records of the current directors of the company, including full names, identity number, occupation, date of most recent election or appointment as director and such further information as required in terms of the Act;
iii. Records of past directors as described in (a) above for a period of seven years;
iv. Copies of reports presented at general meetings of the company for a period of seven years;
v. Notices and minutes of all members' meetings, including resolutions taken by Directors and documents made available to the members in respect of such a resolution – for a period of seven years;
vi. Copies of written communication to all shareholders ;
vii. Minutes and resolutions of every directors' meeting, directors' committees' meeting, audit committee meetings for a period of seven years.

b. Personal information collected from data subjects which is protected by the Protection of Personal Information Act (POPIA):

Information relating to access control into the community scheme, including:

i. Details of all its employees, which details include but not limited to names, surnames, identity numbers, contact details, biometrics, residential and postal address, bank account details, credit and criminal records, all documentation required in terms of and the Disaster Management Act and all applicable labour legislation;

ii. Details of clients, which includes names, surnames, identity numbers and contact details, biometrics residential and postal address, bank account details, source documents pertaining to the instructions received, and all documentation required in terms of FICA and the Disaster Management Act;

iii. Details of contractors or service providers gaining access to the Company or employed for purposes of rendering services to clients including the personal details of representatives of such service providers and contractors including their names, surnames, identity number and contact details.

11. **<u>The right to request information in terms of the Companies Act Section 26:</u>**

a. In terms of Section 26 of the Companies Act 71 of 2008 any person with a beneficial interest in any of the securities of the Company may request the information mentioned in section 24 of the Companies Act.

b. A shareholders' to request information in terms of PAIA is not limited by the provisions of the Companies Act.

c. A may request the following information of the company:

i. Persons other than the Directors and Shareholders may request copies of the company register held by the Directors in terms of section 26 of the Companies Act.

ii. Persons other than the Directors and Shareholders may request any additional information relating to the Company in terms of the PAIA and in terms of this manual.

iii. Third parties not automatically entitled to additional information must bring a formal application in terms of PAIA substantiating the reasons they require such information

12. **<u>Request For Access To Records Of The Company</u>:**

Any interested party who wishes to obtain access to a record of the Company shall apply for access to such a record as indicated herein below**:**

Any record may be requested by making use of the following process:

a) All records may be requested from the Head of the Company in writing and in compliance with the PAIA and this manual;
b) The Company shall not make available any information for inspection and will only, after considering a request for access to information, provide copies thereof to the requester (electronically or otherwise). Only in exceptional circumstances, where it is impossible to provide copies, will inspection be arranged;
c) The Company shall be entitled to demand payment of a request fee and access fee as determined in terms of item 2, part 3 of the regulations promulgated under the PAIA. The aforesaid request and access fees are attached hereto marked as annexure "**A"**.

Note: The Company reserves its rights to withhold copies made or information requested until payment of the aforesaid costs to it has been made by the requester.

d) A request referred to above shall be in writing, substantially in the form of the attached prescribed form C attached as annexure "**B**" to this document, and stating / complying with the following additional requirements:

i. A request shall be delivered via e-mail for the attention of the Information Officer of the company to the address as provided for in this manual;
ii. The full names, physical address and identity number of the requester;
iii. The requester shall state in what capacity he/ she is making this request and whether the application is made on behalf of another party. In such case the other party and the capacity in which the request if made on behalf of the other party needs to be stated;
iv. If the request for information is made on behalf of another person, the requester must provide authorisation for such a request and furnish proof of his/her/its capacity in relation to the person on whose behalf the request is made;
v. Specifying the type of document or information requested (the subject and category within which the document or information falls);
vi. Specification of the date/year of the document if the document is produced periodically or where more than one version of the document is likely to exist;
vii. Indicate which right the requester seeks to protect or exercise with the information requested and provide an explanation why the requested document or information is necessary to protect or exercise his/her/it's right;
viii. Indicate why the record is requested in terms of PAIA and not in terms of the Companies Act;
ix. Whether an electronic or hard copy of document is requested and, if an electronic document is requested (and where it is possible to furnish same electronically) an e-mail address should be provided;
x. Written replies to the request shall be furnished by way of electronic mail, unless indicated otherwise by the requester.

a. Once the Company is in receipt of a request for information, it shall acknowledge the request within 7 (seven) business days, unless otherwise communicated.

b. The request shall thereafter be referred to the head of the Company for consideration and a response.

c. An invoice shall be sent to the requester for payment of the request fee and access fee.

d. The Company shall not make available any personal information to a requester/personal requested without strict compliance with the POPI Act.

e. In terms of section 51(2) of PAIA, this manual must be updated on a regular basis and it is the duty of requesters to conform to the process described in the latest available version of the manual.

ANNEXURE "A"

Request fees and access fees applicable to a request in terms of PAIA

Fees in respect of private bodies

1. The fee for a copy of the manual as contemplated in regulation 9(2)*(c)* is R1.10 for every photocopy of an A4 size page or part thereof.

2. The fees for reproduction referred to in regulation 11(1) are as follows:

a)	For every photocopy of an A4 size page or part thereof	R1.10.
b)	For every printed copy of an A4size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
c)	For a copy in a computer readable form on:	
	(i) stiffy disc	R7.50
	(ii) compact disc	R70.00
d)	(i) For a transcription of visual images, for an A4size page or part thereof	R40.00
	(ii) For a copy of visual images	R60.00
e)	(i) For a transcription of visual images, for an A4-size page or part thereof	R20.00
	(ii) For a copy of visual images	R30.00

3. The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2) is R50.00.

4. The access fees payable by a requester referred to in regulation 11(3) are as follows:

a)	For every photocopy of an A4-size page or part thereof	R1.10
b)	For every printed copy of an A4size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
c)	For a copy in a computer-readable form on:	
	(i) stiffy disc	R7.50
	(ii) compact disc	R70.00
d)	(i) For a transcription of visual images, for an A4size page or part thereof	R40.00
	(ii) For a copy of visual images	R60.00
e)	(i) For a transcription of an audio record, for an A4-size page or part thereof	R20.00
	(ii) For a copy of an audio record	R30.00
	To search for and prepare the record for disclosure, R30.00 for each hour or part of an hour	

	reasonably required for such search and preparation	

5. For purposes of section 54(2) of the Act, the following applies:

a)	Six hours as the hours to be exceeded before a deposit is payable; and	
b)	one third of the access fee is payable as a deposit by the requester.	

ANNEXURE "B"

J752

REPUBLIC OF SOUTH AFRICA

FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))
[Regulation 10]

A. Particulars of private body
The Head:

B. Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below. (b) The address and/or fax number in the Republic to which the information is to be sent must be given. (c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname: .....

Identity number:

Postal address: .....

Telephone number: (.....) ..... Fax number: (.....) .....

E-mail address: .....

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: .....

Identity number:

D. Particulars of record

(a)	Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b)	If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

.....

.....

.....

.....

2. Reference number, if available:

.....

.....

.....

.....

3. Any further particulars of record:

.....

.....

.....

.....

E. Fees

(a)	A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b)	You will be notified of the amount required to be paid as the request fee.
(c)	The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.
(d)	If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

.....

.....

.....

.....

.....

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required:

Mark the appropriate box with an **X**.

NOTES:
(a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:						
	copy of record*		inspection of record			
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):						
	view the images		copy of the images*		transcription of the images*	
3. If record consists of recorded words or information which can be reproduced in sound:						
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)			
4. If record is held on computer or in an electronic or machine-readable form:						
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)	

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

……

……

……

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

……

……

……

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

……..

Signed at …….. this day…… of ……..year …….

……
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE