DATA PROTECTION POLICY

PREAMBLE

CSG RECRUIT ("the Company") has a long and proud tradition of conducting business in accordance with the highest ethical standards and in full compliance with all applicable laws. The Data Protection Policy was developed \to provide clear guidance to all employees and to ensure a consistent approach to business practices throughout the Company. The Company is fully committed to conduct business with the highest level of integrity and we expect your strict adherence to the Data Protection Policy and the law. There will be zero tolerance of non-compliance and any violations will result in swift corrective action, including possible termination of employment. Thank you for your commitment to comply unequivocally with the highest standards of integrity and business ethic.

1. INTRODUCTION

1.1 Inherent in the services to its clients, as well as the management of its employment relationships with its own "employees" (both permanent and on various types of contracts), CAB Holdings continually has access to and needs to process personal data and information relating to individuals .To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Company must comply with the Data Protection Principles. In summary these state that personal data shall:

i) be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

ii) be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

iii) be adequate, relevant and not excessive for those purposes.

iv) be accurate and kept up to date.

v) not be kept for longer than is necessary for that purpose.

vi) be processed in accordance with the data subject's rights.

vii) be kept safe from unauthorised access, accidental loss or destruction.

viii) be transparent at all times.

iv) protect itself from the risks associated with a data breach.

1.2 The Company and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Company has developed the Data Protection Policy.

2. STATUS AND PRINCIPLES OF THIS POLICY

2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Company from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the HR Department. If the matter is not resolved it should be raised as a formal grievance.

2.3 This Policy applies to all Personnel / Staff, directors, Visitors, Members, and contractors / service providers assigned to / contracted to the Company.

2.4 Personnel must be informed about data protection issues, and their rights to access their own Personal Information through the induction process. All directors will receive guidance on data protection during their induction and any contractors should be briefed on the importance of data protection at the start of their assignment, as it relates to safeguarding sensitive Personal Information on a Member, resident, contractor, or employee.

2.5 All Personnel of the Company will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

2.6 Compliance with this Policy is a condition of appointment with the Company and any breach of the Policy may result in disciplinary action, which for serious or deliberate breaches may include dismissal. Knowingly breaching the provisions of POPIA and PAIA may also lead to legal action being taken against the organization and individuals in breach

3. DATA HELD AND PROCESSED

3.1 All personal data shall be;

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;

- obtained only for specific lawful purposes;
- adequate, relevant and not excessive;
- accurate, and kept up to date;
- held for no longer than necessary for the purpose it was obtained for;
- processed in accordance with the rights of data subjects;
- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;
- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client.

3.2 The Company will therefore provide all staff and other relevant parties with a standard form of notification. This will state all the types of data the Company holds and processes about them, and the reasons for which it is processed. The Company will try to do this at least once every three years.

3.3 Personal data that is processed about staff

- Information provided by the member of staff or that the Company gather before or during your employment or engagement with us;
- Information that is provided by third parties, such as references or information from suppliers or another party that we do business with; or
- Information that is in the public domain;
- The types of personal data that we may collect, store and use about you include records relating to your:
    - home address,contact details and contact details for your next of kin;
    - recruitment (including your application form or curriculum vitae, references received and details of your qualifications);
    - pay records, national insurance number and details of taxes and any employment benefits such as pension and health insurance (including details of any claims made);
    - telephone, email, internet, fax or instant messenger use;
    - performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

4. HOW THE COMPANY USE YOUR INFORMATION

The Company will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our privacy notice. We will not process Staff personal information for any other reason.

In general we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:

a. **Staff Address Lists:** to compile and circulate lists of home address and contact details, to contact you outside working hours.

b. **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others that you are absent through sickness, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.

c. **Monitoring IT systems:** to monitor your use of e-mails, internet, telephone and fax, computer or other communications or IT resources.

d. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.

e. **Performance Reviews:** to carry out performance reviews.

f. **Equal Opportunities Monitoring:** to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of the Employer's workforce.

5. DISCLOSURE OF INFORMATION

The Company may disclose your personal information to our service providers who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with the privacy requirements as required by the Protection of Personal Information Act.

The Company may also disclose your information:

- Where we have a duty or a right to disclose in terms of law or industry codes;
- Where we believe it is necessary to protect our rights.

6. INFORMATION SECURITY

The Company legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. The Company will, on

an on-going basis, continue to review our security controls and related processes to ensure that your personal information remains secure.

The Company security policies and procedures cover:

- Physical security;
- Computer and network security;
- Access to personal information;
- Secure communications;
- Security in contracting out activities or functions;
- Retention and disposal of information;
- Acceptable usage of personal information;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

When the Company contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that personal information that the company remain responsible for, is kept secure.

The Company will ensure that anyone to whom we pass your personal information agrees to treat your information with the same level of protection as we are obliged to

7. DATA SUBJECTS RIGHTS TO ACCESS INFORMATION

You have the right to request a copy of the personal information we hold about you. To do this, simply contact us at the numbers/addresses as provided on our website and specify what information you require. We will need a copy of your ID document to confirm your identity before providing details of your personal information.

Please note that any such access request may be subject to a payment of a legally allowable fee

8 RESPONSIBILITIES OF STAFF

8.1 All staff are responsible for:

i) checking that any information that they provide to the Company in connection with their employment is accurate and up to date.

ii) informing the Company of any changes to information, which they have provided i.e. changes of address

iii) checking the information that the Company will send out from time to time, giving details of information kept and processed about staff.

iv) informing the Company of any errors or changes. The Company cannot be held responsible for any errors unless the staff member has informed the Company of them.

8.2 All personal data shall be deemed confidential information, and be handled as such. The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

8.3 Under no circumstances will data or personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary.

8.4 Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols:

- In particular, strong passwords shall be used at all times;
- Passwords shall not be shared under any circumstances;

8.5 If and when, as part of their responsibilities, staff collect information about other people, they must comply with the guidelines for staff.

8.6 All staff will complete training in Data Protection as component of their Induction to employment at the Company.

8.7 When staff are working from home they will ensure that no other persons have any access to their company devices.

8.8 When staff take home their company devices they must ensure that such devices are kept safe and secure at all times when they are away from the company premise.

9 DATA STORAGE

9.1 Paper

Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. This also applies to data stored

electronically which has been printed out for some reason. When not required by such papers should be kept in a locked drawer, safe or cabinet. Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on a printer, and all unwanted paper must be shredded. This information must remain confidential at all times and must not be shared with anyone other than the company administrative staff or duly authorised company employee.

9.2 **Electronic data**

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts:-Data should be protected by strong passwords that are changed regularly and never shared between employees;

- Where data is stored on removable media such as a CD or a DVD these must at all times be locked away securely when not in immediate use;
- All data will only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services;
- All servers containing personal data will be located in secure protected locations away from general office space;
- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager. The Risk and Compliance Manager will be responsible to schedule a minimum of two random tests each year;
- Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;
- All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.
- The company will ensure that all license and fees are up to date and paid.

9.3 **Data Use**

It is acknowledged that personal data 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 data, employees should ensure that screens of their computers are always locked when left unattended;

Personal data will not be shared informally, and in particular it will never be sent by email or without protection with appropriate passwords, where required to be sent by email;

Data shall be encrypted before being transferred electronically. The IT manager together with the Risk Manager will develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties.

10. CLIENT OBLIGATIONS

10.1 Clients must ensure that all personal data provided to the Company is accurate and up to date. The onus is on the Client to inform the relevant person of any changes to their personal information.

11. RIGHTS TO ACCESS INFORMATION (PROMOTION OF ACCESS TO INFORMATION ACT)

11.1 Staff, and other users of the Company have the right to access any personal data that is being kept about them either on computer or in certain files.

11.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing, in the first instance to the Company Data Protection Officer.

11.3 The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 7 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

12 PRODUCTION OF COMPANY INFORMATION

12.1 Information that is already in the public domain is exempt from the POPI Act. It is the Company policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

i) names and contacts of Company Directors

ii) list of staff

iii) Policy documents

iv) Annual accounts

12.2 The Company's internal phone list will not be a public document.

13. SUBJECT CONSENT

13.1 In many cases, the Company can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Company processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions.

13.2 The Company will also ask staff for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The Company will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

13.3 Therefore, all prospective staff will be asked to sign a consent to process data, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

14. PROCESSING SENSITIVE INFORMATION

14.1 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the Company is a safe place for everyone, or to operate other Company policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals. Staff will be asked to give express consent for the Company to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

14.2 The Company will only process sensitive personal information if:

a. we have a lawful basis for doing so, eg it is necessary for the performance of the employment contract; and

b. one of the following special conditions for processing personal information applies:

i. the data subject has given explicit consent.

ii. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject.

iii. he processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.

iv. processing relates to personal data which are manifestly made public by the data subject.

v. the processing is necessary for the establishment, exercise, or defence or legal claims; or

vi. the processing is necessary for reasons of substantial public interest.

15 RETENTION OF DATA

15.1 The Company will keep some forms of information for longer than others. Information should not be kept indefinitely, unless there are specific requirements. No information will be kept for longer than is deemed necessary for the purpose for which it was collected and retained.

15.2 When data is no longer required it should be appropriately destroyed.

16. INFORMATION TRANSFERS OUTSIDE OF SOUTH AFRICA

Section 72 of POPI deals with transfers of personal information outside South Africa or trans border information flows

The Company may transmit or transfer personal information outside South Africa to a foreign country. Personal information may be stored on servers located outside South Africa in a foreign country whose laws protecting personal information may not be as stringent as the laws in South Africa. You consent to us processing your personal information in a foreign country whose laws regarding processing of personal information may be less stringent. It is agreed between the parties that the transfer of such information is necessary for the responsible party to perform in terms of a contract.

17. TIME PERIODS FOR RETENTION OF DATA

17.1 We may retain your Personal Data for a period of time consistent with the original purpose of collection. We determine the appropriate retention period for Personal Data on the basis of the amount, nature, and sensitivity of your Personal Data, the potential risk of harm from unauthorized use or disclosure, and whether we can achieve the purposes of the processing through other means, as well as the applicable legal requirements (such as applicable statutes of limitation).

17.2 After expiry of the retention periods, your Personal Data will be deleted, however we may retain Personal Data where reasonably necessary to comply with our legal obligations (including law enforcement requests), meet regulatory requirements, maintain security, prevent fraud and abuse, resolve disputes, enforce contracts, or fulfil your request to “unsubscribe” from further messages from us. If there is any information that we are unable, for technical reasons, to delete entirely from our systems, we will put in place appropriate measures to prevent any further use of the data.

17.3 We will retain de-personalised information after your account has been closed.

18. DATA SUBJECTS RIGHTS

18.1 Data subjects have the following rights regarding their personal data, which include but are not limited to:

- to withdraw consent to the processing of your Personal Data;
- to access to your Personal Data;
- to request rectification or deletion of your Personal Data;
- to request a restriction on the processing of your Personal Data;
- to object to the processing of your Personal Data;
- the right to data portability (transfer of your Personal Data).
- the right to withdraw consent to processing of your Personal Data.

18.2 To exercise any of their rights, a data subject must contact the company.

18.3 The company will respond to such as request in reasonable time.

19. CHANGES TO THIS POLICY

The Company will update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements and other factors. If we do, we will update the “effective date” at the top of this Privacy Policy. If we make an update, we may provide you with notice prior to the update taking

effect, such as by posting a conspicuous notice on our website or by contacting you using the email address you provided.

20. CONCLUSION

Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Company facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.