PRIVACY AND PROTECTION OF PII

(Control 5.34)

Policy Statement

The Company is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Act, GDPR; POPIA and other regulatory frameworks. The Company needs to process certain information about its staff, third parties and other individuals it has dealings with for administrative purposes.

The policy applies to all staff of the Company. Any breach of the Data Protection Act or the Company Confidentiality and Data Protection Policy is considered to be an offence, and, in that event, the Company disciplinary procedures will apply.

Responsibilities under the Data Protection Act 2018 (POPIA 2021)

The Information Officer is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for the Company.

Compliance with data protection legislation is the responsibility of all staff of the Company who process personal information.

Staff are responsible for ensuring that any personal data for which they are responsible is kept accurate and up to date.

If any staff member is in doubt about any Confidentiality or Data Protection issue, they should consult the Information Officer.

Processing of Personal Data

All personal data is processed in accordance with the following principles:

- Personal data shall be processed fairly and lawfully.
- Processing personal data must make reasonable efforts to ensure that data subjects are informed of the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
- Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.
- Data obtained for specified purposes must not be used for a purpose that differs from those.
- Personal data shall be adequate, relevant, and not excessive in relation to the purpose for which it is held.

- Information, which is not strictly necessary for the purpose for which it is obtained, will not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Data, which is kept for a long time, must be reviewed, and updated, as necessary. It is the responsibility of staff to ensure that data held by the Company is accurate and up to date. Completion of an appropriate registration or application form (for example) will be taken as an indication that the data contained therein is accurate. Individuals should notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is noted and acted upon.
- Personal data shall be kept only for as long as necessary according to the company data retention policy
- Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

Respecting the Rights of Data Subjects

The Company will respect the rights of Data Subjects, in respect of information held about them. Specifically, the Company will:

- Respond to access requests regarding the nature of information held and to whom it has been disclosed. Under the POPIA individuals are entitled to request access to their personal data.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Ensure that significant decisions that will affect Data Subjects are not taken solely by an automated process.

Obtaining Consent

Wherever possible, personal data or sensitive data will not be obtained, held, used, or disclosed unless the individual has given consent. The Company understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

In most instances consent to process personal and sensitive data is obtained routinely by the Company (for example when a beneficiary signs a registration form or when a new member of staff signs a contract of employment). Any Company forms (whether paper-based or web-based) that gather data on an individual will contain a statement explaining what the information is to be used for and to whom it may be disclosed.

If an individual does not consent to certain types of processing (such as direct marketing), appropriate action will be taken to ensure that the processing does not take place.

Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. Staff will form a judgement based upon the sensitivity and value of the information in question. All personal data will be kept securely. All data disposals will be done securely either physical or electronically.

In case of a personal data breach, the company will have to notify the organisation responsible for this purpose, the Data Protection Authority (DPA) ('National supervisory authority, acting with complete independence, responsible for monitoring the application of data protection rules at the national level'), within 72 hours after having detected the violation.

Right of Access to Personnel Data

Staff have the right to access any personal data which are held by the Company in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Company about them.
Any individual who wishes to exercise this right should apply to the head of HR.

Disclosure of Data

Staff must ensure that personal data is not disclosed to unauthorised third parties. All staff must exercise caution when asked to disclose personal data held on another individual to a third party.

Disclosure of the information is relevant to, and necessary for, the conduct of company business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them to the member of staff concerned.

Personal data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent
- Where the disclosure is in the legitimate operations of the company
- Where the institution is legally obliged to disclose the data
- Where disclosure of data is required for the performance of a contract
- Personal data can be disclosed under certain circumstances

Staff are asked to contact a senior manager for guidance if any of these circumstances arise (excepting cases of immediate serious harm or life and death where the employee must use their judgement):

- to safeguard national security.
- prevention or detection of crime including the apprehension or prosecution of offenders.
- assessment or collection of tax duty.
- discharge of regulatory functions (includes health, safety, and welfare of persons at work).
- to prevent serious harm to a third party.
- to protect the vital interests of the individual, this refers to life and death situations.

Retention and Disposal of Data

The Company discourages the retention of personal data for longer than required according to data retention policy. (*POPIA – Section 14*)

Clients - In general, electronic records containing information about individuals are kept indefinitely and information would typically include name and address function and other sundry information.

Staff - In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held and leaving salary. Other information relating to individual members of staff will be kept by the head of HR for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Recruitment - Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Do not pass personal details to cold calling recruitment agents or other service providers seeking employee details including names, contact details, roles, skills, and personal opinions.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).