1.0 TITLE

Privacy Procedure

2.0 SCOPES

This policy and procedure pertain to the collection of personal information, irrespective of its origin, as well as to the storage, handling, access, modification, management, transfer, use, and disclosure of personal information, regardless of the time of its collection.

This policy is applicable to all company staff/employees who are involved in accessing, using, or managing personal information, as well as those who handle inquiries or complaints regarding personal information, within the scope of company-related activities.

3.0 RESPONSIBILITIES

3.1 Employees are responsible in ensuring that their work practices align with this policy and any associated procedures.

3.2 Employees are required to promptly report any privacy breaches to a designated privacy officer upon becoming aware of them.

3.3 Staff has a responsibility to take reasonable steps to ensure that information is accurate, up-to-date, and complete.

3.4 Management is responsible for authorizing access to data for staff or other individuals within their areas of authority.

3.5 Suppliers and customers needing access to company administrative data must include appropriate provisions mandating the maintenance of privacy and security of the company's data.

3.6 Employees who contravene this policy may face disciplinary measures for misconduct and/or performance issues, in accordance with the relevant administrative procedures applicable to their employment.

4.0 REFERENCE

4.1 Personal Data Protection Act 2010

5.0 DEFINITION

5.1 **Personal Information:** means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not, or as otherwise defined by applicable data protection laws.

5.2 **Sensitive Information:** Sensitive information includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, biometric information, biometric templates, health information about individual and genetic information.

5.3 **Data Processors:** Data Processor or Service Provider means any natural or legal person who processes the data on behalf of the Data Controller.

Confidential- For Internal Use Only

- Notice: This document is considered "UNCONTROLLED COPY" when it exists in any printed form, except when affix with "CONTROL COPY" stamp. Refer to PPSB Document Control Center filling for the current master version of this document

FOR REFERENCE ONLY

Confidential- For Internal Use Only

- Notice: This document is considered "UNCONTROLLED COPY" when it exists in any printed form, except when affix with "CONTROL COPY" stamp. Refer to PPSB Document Control Center filling for the current master version of this document

FOR REFERENCE ONLY

6.0 PURPOSE

The objective is to ensure the protection of an individual's privacy and to undertake all reasonable measures to safeguard personal information.

7.0 Collection of Personal Information

PPHB will solely gather Personal Information about an individual through fair and lawful methods and only when the information is essential for the following purposes:

i. To adhere to legal requirements;
ii. To furnish data to government agencies as mandated by law;
iii. To provide suitable services and care;
iv. To lawfully communicate with a designated representative and to contact family members.

We refrain from collecting or retaining sensitive information unless it is provided by employees, employees consent to its collection, and the information is reasonably necessary for our business or activities.

Access and security for personal information records

Access and security safeguards are crucial for safeguarding personal privacy. Access to personal information is restricted to staff only when necessary for work purposes, and they should only access personal information if there is a legitimate work-related reason to do so. Personal information must be safeguarded against loss, unauthorized access, modification, disclosure, or misuse.

Holding and securing personal information

PPHB will store all employee's personal information in both hard copy and digital formats, both on-site and with several third-party providers. All hard copy materials are secured using locked filing cabinets or office security measures. Similarly, all digital materials are protected using file access controls.

PPHB maintains employees' personal information solely for the duration necessary for the intended purpose or as mandated by law. If there is no longer a legitimate need to retain such information PPHB will take reasonable measures to either de-identify or securely destroy it.

Confidential- For Internal Use Only

- Notice: This document is considered "UNCONTROLLED COPY" when it exists in any printed form, except when affix with "CONTROL COPY" stamp. Refer to PPSB Document Control Center filling for the current master version of this document

FOR REFERENCE ONLY