WORKPLACE PRIVACY POLICY

1. Purpose and Application

1.1. **Yovich Hayward Pevats Johnston Limited (YHPJ)** ("**the Company**") collects, uses, stores, and potentially discloses personal information of individuals in the workplace for purposes related to the individuals' engagement, be it as employees, applicants for employment, contractors, volunteers, or visitors ("workplace participants"). This policy sets out the general principles that guide and govern the Company's collection, use, storage, and disclosure of personal information in accordance with the Privacy Act 2020 ("**the Act**") and its subsequent amendments. It applies to all of the Company's workplace participants.

1.2. The terms and definitions (for example, "personal information", "information privacy principles", "serious harm", etc.) referred to in this policy shall have the same meaning and interpretation as those referred to in the Act. Where this policy refers to "employees", this shall also include other workplace participants, unless the context requires otherwise.

2. Employer Responsibilities

2.1. The Company will abide by its obligations under the Privacy Act 2020 and its subsequent amendments (including but not limited to the Information Privacy Principles stated therein, and any applicable Codes of Practice), which includes responsibility for:

a. Informing individuals what the Company does with their personal information and why;

b. Collecting only the relevant personal information the Company needs from individuals in order to provide our services and/or in connection with the lawful functions and/or activities of the Company, and the individuals' relationships with the Company (e.g. all and any employment-related purposes);

c. Only using personal information if the Company is reasonably sure it is accurate;

d. Keeping personal information safe and secure from loss and/or unauthorised access, use, modification, or disclosure;

e. Providing individuals' rights to access, review, and correction of their personal information;

f. Investigating potential interferences with or breaches of privacy rights; and

g. Notifying the Privacy Commissioner and affected individuals as soon as practicable after becoming aware of the occurrence of a notifiable privacy breach.

3. Employee Responsibilities

3.1. Employees are responsible for:

a. Disclosing all relevant information about them as part of their pre-employment application process and any matter relevant to their employment;

b. Providing the Company with up-to-date contact information;

c. Ensuring the privacy of other employees, customers, clients, agents, contractors or any other person or entity that has dealings with the Company is protected and is not breached;

d. Immediately notifying the Company of any involvement in or knowledge of any actual or potential interferences with or breaches of privacy rights.

e. Complying with all other obligations set out in the Act, this policy (including any delegated activities referred to in section 4, below), the applicable employment agreement, and/or any other relevant Company policies.

4. Responsibilities and Processes regarding the collection, use, disclosure, and storage of personal information

4.1. The below information is intended to reflect a summary of the provisions/Information Privacy Principles of the Privacy Act 2020 and its subsequent amendments, and how they apply to the Company. In the event of an inconsistency between the provisions of this policy and those of the Privacy Act, the Act will prevail.

4.2. Collection of personal information

a. The Company (via its authorised agents/representatives) will only collect personal information for lawful purpose/s in connection with the functions or activities of the Company and as far as is necessary for such purpose/s. A "lawful purpose" in respect of the collection of information is any purpose that is relevant in respect of the relationship between the Company and the individual (e.g. this can be a workplace participant, customer, etc.). For the avoidance of doubt, the Company does not "*collect*" personal information if information is provided to it in an unsolicited manner.

b. The Company will collect personal information directly from the individual, and it will take reasonable steps to ensure that the individual is informed about the fact of the collection, its purpose, the intended recipients of the collected information, the agencies collecting/holding/using the personal information, the individual's rights regarding access to and correction of their personal information, and/or any other relevant matters.

c. However, the Company may not be required to abide by the obligations in sub-section b. and may collect the information from other sources (e.g. third parties) and without notifying the individual, if the Company believes on reasonable grounds that:

i. Doing so is authorised by the individual concerned or would not prejudice the interests of the individual concerned; or

ii. Notification of and collection from the individual concerned would prejudice the purpose of the collection (for example, in the context of employment investigations, and/or matters warranting and justifying covert surveillance measures); or

iii. This is necessary for the purpose of avoiding prejudice to the maintenance of the law by any public sector agency (including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences), or the enforcement of a law that imposes a pecuniary penalty, or the protection of public revenue; or for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

iv. In respect of other grounds referred to in the Act.

4.3 Use of personal information

a. The Company may use collected personal information only for the purpose/s the information has been collected for (including any directly related purpose/s), or any other purposes authorised by the individual concerned.

b. However, the Company may use the information for other purposes if the Company believes on reasonable grounds that the use of the information:

   i. Does not identify the individual concerned; or

   ii. Is publicly available; or

   iii. Is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences, or for the enforcement of a law that imposes a pecuniary penalty, or for the protection of public revenue, or for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

   iv. Is necessary to prevent or lessen a serious threat to public health or public safety, or the life or health of the individual concerned or another individual; or

   v. in any other circumstances allowed by the Act or any other relevant law.

c. For the avoidance of doubt, the Company may use personal information from and/or about employees for any purpose that is directly or indirectly related to the employee's employment, unless the Company and the particular employee have expressly agreed otherwise. This is inclusive of, without limitation, the following purposes:

   i. To verify an individual's identity;

   ii. To undertake employment checks in relation to an individual (including authorised reference checks);

   iii. To conduct any employment-related processes, in relation to or about the individual or any other individual; and

   iv. Any other purposes authorised by the individual and/or the Act (or any other applicable law), for example to market or provide the Company's services and products, invoicing and collection of monies owed to the Company, or for the protection or enforcement of the Company's legal rights and interests.

d. The Company will take reasonable steps to ensure that the used personal information is accurate, current, complete, and not misleading.

4.4 Disclosure of personal information

a. The Company will not disclose personal information to any other person and/or agency, unless such disclosure accords with the purpose it has been collected for (or is directly related to such purpose), or the disclosure is authorised by the individual concerned (for example, disclosures to authorised representatives), or the information is publicly available, or the individual is not identified by the disclosure.

b. Examples of such disclosures may include any disclosures directly or indirectly related to the individual's employment, or application for employment (for example, reference checks, background checks via the Ministry of Justice, New Zealand Police, or any other law enforcement agencies, credit checks via banks or other finance institutes, etc.), or as may be required by law from time to time.

c. However, the Company may also disclose the information, other than in the circumstances referred to in sub-sections a. and b., if the Company has reasonable grounds to believe that the disclosure is necessary for the purpose of:

   i. Facilitating the sale or other disposition of a business as a going concern; or

   ii. Avoiding prejudice to the maintenance of the law by any public sector agency (including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences), or for the enforcement of a law that imposes a pecuniary penalty, or for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation), or for enabling an intelligence and security agency to perform any of its functions, or for protecting of public revenue; or

   iii. Preventing or lessening a serious threat to public health or public safety or the life or health of the individual concerned or another individual.

d. Where the disclosure of personal information is being made to a foreign person or entity (i.e. a person or entity that is not physically present in New Zealand, and not an ordinary resident of New Zealand, and – in the case of an entity- that is not established under the laws of New Zealand and is not managed/controlled from New Zealand) the Company will carry out necessary due diligence to ensure that it has reasonable grounds to believe that the foreign person or entity meets at least one of the criteria of Information Privacy Principle 12 of the Act. Essentially, these criteria ensure that any disclosure of personal information outside of New Zealand will be subject to privacy safeguards that are comparable to those under the Act.

e. For the avoidance of doubt, where another entity (either located within or outside of New Zealand) holds or processes personal information on behalf of the Company (for example, cloud storage), the information is regarded as being held by the Company itself and accordingly, this does not constitute a disclosure of information.

f. The Company will take reasonable steps to ensure that the disclosed personal information is accurate, current, complete, and not misleading.

4.5 Protecting and holding personal information

a. The Company will take reasonable steps to protect personal information from loss, unauthorised access, use and/or disclosure, or any other misuse.

b. The Company will not retain personal information for longer than is required for the purposes for which the information has been collected or may be used. In general, however, personnel files will be kept for up to six (6) years (after the ending of the relationship) before it will be safely destroyed.

c. Personal information related to applications for employment with the Company may be kept for up to one (1) year before it will be destroyed.

4.6 Accessing and correcting personal information

a. Unless stated otherwise in the Act, workplace participants and other individuals are entitled to request confirmation from the Company whether it holds personal information about them, and they may also request access to and/or correction of their personal information.

b. The Company will provide reasonable assistance to an individual concerned (or their authorised representative), who wishes to or is making a request under subsection a., above. The Company may require evidence to confirm the identity and/or authority of the requesting person.

c. Requests in accordance with this clause should be made in writing (email suffices) to the Company's Privacy Officer, and requests should provide evidence of the identity and authority of the requesting person, and details of the request (for example, any specific information that is requested to be accessed and/or provided).

d. The Company may on a case-by-case basis charge reasonable costs to the requesting individual in relation to the provision of requested personal information, or a correction thereof, or any assistance in the above respects, and the Company will notify the requesting individual of any such charges before processing the request. The Company may request the payment of any such costs in advance of processing an individual's request.

e. If the Company does not hold the requested information, but believes that another agency holds the requested information, the Company will 'transfer' the request to the other agency within ten (10) working days after the day it receives the request, unless it has good reasons to believe that the individual does not wish the request to be transferred to such other agency. In either case, the Company will inform the requesting individual.

f. Except for the event of a transfer, the Company will respond to a request under this clause within twenty (20) working days after the day it receives the request and in accordance with the requirements of the Act (see section 44 of the Act for requests for access to information, and section 63 of the Act for requests for correction of information).

g. The aforementioned time limits may be extended in accordance with the Act (section 65 of the Act), in which case the Company will notify the requesting individual accordingly within twenty (20) working days after the day it receives the request.

h. With regard to a request for access to personal information, the Company may refuse access to personal information in accordance with the Act (see sections 49 to 53 of the Act), for example, where a refusal is necessary for the protection of an individual's health or safety, or where the information is evaluative material or a trade secret.

5 No privacy expectations in respect of use of Company equipment

5.1 For the avoidance of doubt, the Company may collect, use and disclose any personal information that has been stored on, or received/sent by any equipment that has been provided to employees, for any employment-related purpose, or any other purpose related to the protection or enforcement of the Company's legal rights and interests. This includes any form of temporary and/or permanent overt and/or covert surveillance.

5.2 The Company's rights in this respect will not be limited by the circumstance that such equipment may have been issued for reasonable personal use (in addition to work-related use).

5.3 Company provided equipment incudes, without limitation, telephones, computers/laptops, tablets, other devices, swipe cards, company vehicles, GPS trackers and data, work-email accounts, work-phone data, etc. Any information held on such equipment and related data is generally not subject to an employee's privacy rights, and employees must not hold any expectations of privacy in respect of their use of equipment that is provided by the Company.

6 Complaints process and internal reporting of concerns or interferences with privacy rights/privacy principles

6.1 Workplace participants must immediately inform the Company, through its Privacy Officer, of any involvement in or knowledge of any (actual or potential) concerns or interferences with an individual's privacy rights and/or the corresponding privacy principles, so that the Company can take steps to investigate, mitigate, and/or resolve such concerns or interferences. Concerns or interferences must be reported to the Company regardless of the concern or interference being a breach involving potential or actual serious harm that may require the Company to proceed as outlined in section 8, below.

6.2 Workplace participants are also strongly encouraged to raise any complaint in relation an interference or breach of their own privacy rights with the Company (via its Privacy Officer). Whilst the Company encourages the internal reporting of privacy-relate complaints, as this will normally enable a quicker and less stressful resolution, all workplace participants are nevertheless entitled to seek independent advice and/or complain to the Privacy Commission. Advice can be sought and a complaint to the Privacy Commission can be made via its website at https://privacy.org.nz/your-rights/making-a-complaint/.

6.3 Any concerns or interferences or concerns referred to in sub-sections 6.1 and 6.2, above, may relate to, for example, any unauthorised (including accidental) access to, or use, disclosure, alteration, loss or destruction of personal information, or any action that may prevent the Company from temporarily or permanently accessing the personal information).

6.4 If it is not possible or practicable for workplace participants to inform the Privacy Officer, they must inform their Manager.

6.5 The information provided to the Company/its Privacy Officer should include all relevant details, i.e. what has happened, when it has happened, and who was involved (witnesses, etc.). The Company may require such information to be provided in writing, and unless the protections of the Protected Disclosures Act 2000 may apply, the informing itself and the provided information are not subject to confidentiality.

7 Breach Response Process

7.1 Upon receipt of a privacy-related concern, interference or complaint, the Company will liaise with the relevant parties to investigate the matter in order to ascertain whether any such concern, interference or complaint may be substantiated, and whether any further steps may be warranted, for example mitigation of the impacts of any established interference or breach, remediation and resolution, and/or notification of privacy breaches in accordance with section 8 of this policy.

8 Notification of Privacy Breaches (to Privacy Commission and others)

8.1 The Company may be required to notify the Privacy Commission and any affected individuals, and potentially the public, of particular privacy breaches ('notifiable privacy breaches').

8.2 A privacy breach that needs to be notified in this respect is any unauthorised or accidental access to, disclosure, alteration, loss or destruction of personal information, or an action that prevents the Company from accessing the information on either a temporary or permanent basis, which has caused or is likely to cause 'serious harm' to affected individuals.

8.3 In order to assess whether or not such privacy breach may have occurred, and whether the Company's obligation to notify the Privacy Commission and any affected individuals is triggered, workplace participants must immediately inform the Company's Privacy Officer of any involvement in or knowledge of an actual or potential privacy breach, as per section 6 of this policy. Failure of an employee to notify the Company of any involvement in or knowledge of an actual or potential privacy breach, may constitute serious misconduct and may potentially result in disciplinary action up to and including termination of employment.

8.4 The assessment of whether a privacy breach may be notifiable rests exclusively with the Company. The Company will consider the following factors as part of its assessment:

a. Whether any action has been taken to reduce the risk of harm following the breach;

b. Whether the personal information is sensitive in nature;

c. The nature of the harm, if any, that may be caused to affected individuals;

d. The person or body that has obtained or may obtain personal information as a result of the breach (if known);

e. Whether the personal information is protected by a security measure (for example encryption); and

f. Any other relevant matter.

8.5 The Company will notify the Privacy Commission as soon as practicable after becoming aware of a notifiable privacy breach.

8.6 The Company will notify affected individuals as soon as practicable after becoming aware of a notifiable privacy breach, unless it can decide not to notify or delay notification due to a genuine belief that notification would likely:

a. Endanger the safety of any person; or

b. Prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

c. Prejudice the maintenance of the law by any public sector agency, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

d. Reveal a trade secret.

9 Privacy Officer Functions

9.1 The Company has a Privacy Officer to assist with its obligations and functions under the Act.

9.2 The functions of the Privacy Officer are delegated to the incumbent of the position of YHPJ's Compliance Administrator currently Taylah Sowry, 23 Rathbone Street, Whangarei; Phone (09) 470 0400 and email address: yhpjprivacyofficer@yhpj.co.nz The Company may, at its sole discretion, delegate the functions of the Privacy Officer to one or more other individuals within the company, or any external provider.

9.3 Requests for access to personal information, or correction thereof, or any complaints in respect of privacy matters, or information and/or concerns regarding actual or potential interferences with or breaches of privacy rights must be made to the Privacy Officer. Should this not be possible or practicable in the circumstances, requests/complaints should be made to the Managing Director of the Company.

9.4 The Privacy Officer (or any other authorised person within the Company) will liaise with the relevant internal and/or external stakeholders in respect of privacy matters (for example, management, IT staff/consultants, insurance providers, legal advisors, personnel from the Privacy Commission, etc.

10 Further Information

Further information about the Privacy Act 2020, other relevant regulations, the Privacy Commission, its complaints procedures, your legal rights in respect of privacy, etc., can be found via the following links:

10.1 Privacy Act 2020**:** http://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html

10.2 Office of the Privacy Commissioner: https://www.privacy.org.nz/the-privacy-act-and-codes/the-privacy-act/

11 Policy Amendments

The Company is entitled to amend this policy from time to time at its sole discretion and all employees are required to observe such lawful amendments.