PRIVACY POLICY (the "Privacy Policy")

Jennifer Spreckley, operating as an individual or as Kingsway Pilates ("**we**", "**our**" or "**us**"), who provide Services, as defined in our **Terms of Use** is committed to user (the "**User**", "**You**" or "**Your**") privacy and to protecting the confidentiality of the personal information of Users that we collect and handle through Users' use of any one or more of the App, our Website or User Account (as **App, Website** and **User Account** are defined in the Terms of Use).

We subscribe to apps including but not limited to, the Jane App, a clinic management platform, which has its own privacy policy that can be accessed here: https://jane.app/legal/privacy-policy. In the case of a conflict between the Jane App privacy policy and this Privacy Policy, this Privacy Policy prevails.

Jennifer Spreckley, operating as an individual or as Kingsway Pilates, is considered an organization ("**Organization**") under Canada's federal privacy legislation, the *Personal information Protection and Electronic Documents Act* ("**PIPEDA**") in respect of the User personal information it collects, uses and discloses.

Personal information (PIPEDA)
Under the federal private sector privacy legislation, PIPEDA, Personal information is defined as information about an identifiable individual. We subscribe to the Jane App to collect your name, email address or contact information for electronic text messaging, wellness history and outcome measures; we may also use a survey and intake form.

Accountability for Personal information
As an organization under PIPEDA we are responsible for the personal information we collect, use and disclose as a result of Your use of one or more of the Website, App, Content and User Account. We only collect Your personal information with Your consent, or as may be permitted or required by law. If you do not consent to our collecting, using and disclosing your personal information please discontinue your use of our App, Website and User Account. By using any one or more of our App, User Account, Content and Website, You consent to permit our collection, use and disclosure of Your personal information in accordance with this Privacy Policy and our Terms of Use. The purposes for our collection, use and disclosure of Your Personal information are described below.

Privacy Officer
If you have questions about this policy, please contact our privacy officer:

Jennifer Spreckley
26 Aylesbury Road, Etobicoke ON M9A 2M5
Privacy Officer contact: *kingswaypilates@gmail.com*

Purposes for Collecting Personal information
We collect personal information for purposes related to our provision of the Services (as defined in our Terms of Use). In particular, personal information may be collected for the following purposes:

1. Providing you with the Services.
2. Communicating with you about your health and wellness, tracking your progress and scheduling Services, whether by telephone, videoconference, messaging, live videochat or correspondence and in real-time or otherwise.
3. For quality purposes, which may include but are not limited to one or more of evaluating, measuring and analyzing whether we are meeting our standards in providing the Services.
4. To handle payments.
5. For marketing purposes.
6. To display content from external platforms such as the App.
7. To train our employees and agents.
8. To analyse and improve the quality of the Services we provide.

9. To keep in touch with you.
10. To maintain and provide the necessary technological infrastructure to support the provision of the Services.
11. Manage data and survey collection.
12. Manage contacts.
13. For administrative purposes related to any of the above purposes.

More information about the types of personal information collected by the App can be found in the *Jane App* privacy policy, available here https://jane.app/legal/privacy-policy. As the User, you are in sole control as to whether you permit the App to collect information from your device including but not limited to your geographic location, microphone, camera and speech recognition permissions. We will limit our use and disclosure of your personal information to that which is needed to provide the Services and for the purposes identified above unless you expressly authorize us otherwise. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, Your consent will be required before the information can be used for that purpose. We are not responsible for, and disclaim all liability arising from, your provision to us of any information via your choosing to enable your speech recognition, microphone or camera functions on the device you use to access any one or more of our Website, the App, User Account and Content.

Consent for the Collection, Use and Disclosure of Personal information

Under PIPEDA, Organizations require consent in order to collect, use, or disclose personal information. By using one or more of the Website, Content, User Account and App, you consent to our collection, use and disclosure of your personal information for the purposes listed above. There are some cases where we may collect, use or disclose Personal information without Your consent, but such cases are limited to those permitted or required by law.

Express consent

If You, as a User, wish Your lawyer, insurance company, family member, employer, landlord or other third-party individuals or agencies to have access to Your Personal information held by us You must give us Your written consent by contacting our Privacy Officer at the address above. Any written consent must be signed, dated and witnessed and must be current and time-limited to 90 days.

No Consent

There are certain activities for which Your consent is not required for us to use or disclose personal information. These activities are permitted or required by law. For example, we do not need consent from Users to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, the App, the Website, our programs and Services
- Get paid
- Engage in quality improvement, error management, and risk management activities
- Train our employees, agents and others
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations

If Users have questions about using and disclosing personal information without consent, please contact our Privacy Officer at the address above.

Withholding or Withdrawal of Consent

If consent is sought, a User may choose not to give consent ("**withholding consent**"). If consent is given, a User may withdraw consent at any time, but the withdrawal must be recorded and communicated to us and is not retroactive. This means that information already communicated to us will have been collected with consent but going forward, no further collection will occur. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice. If You withdraw or withhold Your

consent You cannot continue Your Use of any one or more of our App, Content, User Account and Website.

Limiting Collection of Personal information
The amount and type of personal information that we collect directly from the User is limited to that which is necessary to fulfill the purposes identified. Information is collected directly from the User, unless PIPEDA, or another law permits or requires collection from third parties. Personal information and is only collected as needed to provide the Services and fulfill the purposes.

Limiting Use, Disclosure and Retention of Personal information
Personal information is not used for purposes other than those for which such information was collected, except with the consent of the User or as permitted or required by law. Any of our employees or agents may use the information, except only as needed within the limits of their individual roles. Our employees and agents do not read, look at, receive or otherwise use personal information unless they have a legitimate "need to know" as part of their role. They seek assistance from our privacy officer as needed and are taught to keep personal information secure and confidential and may be asked to sign confidentiality agreements and attend training in respect of their handling of such personal information.

Disclosure
Personal information is not disclosed for purposes other than those for which such information was collected, except with the consent of the User or as permitted or required by law. Personal information may only be disclosed within the limits of each employee's or agent's individual's role. The limitation described above relating to each employee's or agent's role applies.

Retention
Personal information is retained as required by law and to fulfill the purposes for which the information is collected. Information that is no longer required to fulfill the identified purposes is securely destroyed, erased, or made anonymous.

Accuracy of Personal information
We will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate or inaccurate information may be used to make a decision about a User.

Safeguards for Personal information
We have put in place safeguards for the personal information we hold, which include:

- Physical safeguards (such as locked doors and cabinets and restricted access to servers)
- Organizational safeguards (such as permitting access to information by employee or agents on a "need-to-know" basis only, confidentiality agreements and privacy training); and
- Technological safeguards (such as the use of passwords, encryption, and audits)

We take steps to ensure that the personal information we hold is protected against theft, loss and unauthorized use or disclosure. We require anyone who collects, uses or discloses personal information on our behalf to be aware of the importance of maintaining the confidentiality of the information. This is done through the signing of confidentiality agreements, privacy training, and contractual means. Care is used in the secure disposal or destruction of personal information, to prevent unauthorized persons from gaining access to the information.

Openness about Personal information
Information about our policies and practices relating to our management of personal information are available to the public, including:

- Contact information for our Privacy Officer (above), to whom complaints or inquiries can be made;
- The process for obtaining access to personal information we hold, and making requests for its correction;
- A description of the type of personal information we hold, including a general account of our uses and disclosures; and

- A description of how a User may make a complaint about our privacy practices, to us, or to the Privacy Commissioner of Canada (see below).

User Access to Personal information

Users may make written requests to have access to, and correction of, their records of personal information. We will respond to a User's request for access within reasonable timelines and costs to the User, as governed by law. We will take reasonable steps to ensure that the requested information is made available in a format that is understandable. Users who successfully demonstrate the inaccuracy or incompleteness of their personal information may request that we amend their information. In some cases, instead of making a correction, Users may ask to append a statement of disagreement to their file.

Please Note: In certain situations, we may not be able to provide access to all of the personal information we hold about a User, such as where the access could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege, or in other situations as permitted by law and described below (See Denying User Access to Records).

User Requests to Access their own Information

With limited exceptions, we are required by law to respond within 30 days to Users who make written requests to access their records of personal information (subject to a time extension of up to an additional 30 days if necessary and with notice to the person making the request).

a. Requests to Access

i. User requests for their own information should be made in writing.

ii. Users may request whether the Organization holds their Personal information and the sources of this information and whether it has been used or disclosed.

iii. Requests must be specific enough to allow us to find your Personal information. We may work with the User to locate the desired information. If our records are difficult to read and interpret, or use shorthand or short forms, Users will be encouraged to review the records with us so the information can be explained. Users seeking access may be asked to provide identification in order to verify their identity prior to being given access.

iv. We provide access at minimal or no cost, depending on the request.

v. If a User wishes to read the original record, someone from our organization must be present to ensure the records are not altered or removed. Users may not make notes on the original record or remove originals from the record or otherwise alter their records.

vi. If a User requests a copy of a record, copies may be given and minimal fees may be applied.

vii. The original written User request for access will be placed with the User's records and must contain the following:

- A description of what information is requested
- Information sufficient to show that the person making the request for access is the User or other authorized person
- The signature of the User or other authorized person and a witness to the signature
- The date the written request was signed

viii. A notation shall be made in the User's record (e.g., a handwritten note) stating:

- What information or records were disclosed
- When the information or records were disclosed
- By whom the information or records were disclosed

ix. If an individual requests access to the User's information on behalf of the User a signed consent from the User will be necessary and the consent must have been signed by the User within 90 days prior to the request.

b. Denying User Access to Records

In certain situations, we may refuse a User's request for access to all or part of a record. Exceptions to the right of access requirement must be in accordance with law. Reasons to deny access to a record (or part of a record) may include:

- the information is subject to a legal privilege that restricts disclosure to the individual
- disclosure would reveal personal information of another individual, unless that information can be severed from the record
- the information cannot be disclosed for legal, security or commercial proprietary reasons
- if granting access could reasonably be expected to result in a risk of serious bodily harm to the individual or another person;
- the information was generated in the course of a dispute resolution process;
- or the purpose of a legal proceeding; or
- the information is prohibitively costly to provide.

A User who requests access will not be denied access if the requester needs the information because the requester's life, health or security is threatened.

Users must be told if they are being denied access to their own health records. In such cases, Users have a right to complain to the Privacy Commissioner of Canada, and must be told of this right and how to reach the respective Commissioner's office.

c. Correction of Records

Users may request that their information be corrected if it is inaccurate or incomplete. Such requests must be made in writing and must explain what information is to be corrected and why. We have an obligation to correct personal information if it is inaccurate or incomplete for the purposes.

We must respond to requests for correction within 30 days (or seek an extension of up an additional 30 days but only if we have let the User know, in writing). Corrections are made in the following ways:

- Striking out the incorrect information in a manner that does not obliterate the record, or
- If striking out is not possible:
    - labelling the information as incorrect, severing it from the record, and storing it separately with a link to the record that enables us to trace the incorrect information, or
    - ensuring there is a practical system to inform anyone who sees the record or receives a copy that the information is incorrect and directing that person to the correct information.
- We may also add correct information.

The record will not be corrected if the record was not originally created by us, or the record consists of a professional opinion which was made in good faith. We have discretion regarding correction of our records that contain the User's Personal information and correction requests may not always be granted. If we choose not to correct a record, the User must be informed in writing. The User will have the choice to submit a statement of disagreement, which will be scanned or otherwise attached to the record and released any time the information that was asked to be corrected is released. In these cases, Users have a right to complain to the Privacy Commissioner of Canada, and the contact information is below.

Challenging Compliance with Our Privacy Policy and Practices

Any person may ask questions or challenge our compliance with this policy or with PIPEDA by contacting our Privacy Officer or the individual that provided the Services to you. We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal information. We will inform Users who make inquiries or lodge complaints of other available complaint procedures. We will investigate all complaints. If a complaint is found to be justified, we will take appropriate measures to respond.

The Privacy Commissioner of Canada oversees compliance with privacy rules and PIPEDA. Any individual can make an inquiry or complaint directly to the Commissioner by writing or calling:

Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau, Quebec K1A 1H3
Canada
Toll-free: 1-800-282-1376
Phone: (819) 994-5444
TTY: (819) 994-6591

Signed:  Date: _____

Print Name: _____