

<b>POLICY COR # P- 10</b>	<b>APPROVED BY:</b> <b>The CEO</b>
<b>SECTION: Corporate Administration</b>	<b>APPROVAL DATE: December 8, 2012</b>
<b>ISSUED BY: Corporate Office</b>	<b>REVISED:</b>
<b>TITLE: Privacy Policy</b>	<b>CROSS-REFERENCE:</b>
	Page 1 of 7

**PURPOSE:** In order to provide specialized support and clinical service to our clients, it is essential that we collect personal information from each client to inform their individualized client support plans. This policy has been developed to clarify the process for the collection, handling and disclosure of personal information to ensure compliance with all relevant requirements as defined under the *Personal Information Protection and Electronic Documents Act (PIPEDA); (Ontario's Personal Health Information Protection Act, PHIPA or the privacy Laws )*.

**COMMITMENT:** We are committed to providing our clients and customers with exceptional service. Providing our service involves the collection, use and disclosure of some personal information about our clients and customers. As a result, protecting their personal information is one of our highest priorities.

While we have always respected our clients' and customers' privacy and safeguarded their personal information, we have strengthened our commitment to protecting personal information as a result of the *Personal Information Protection and Electronic Documents Act (PIPEDA and Ontario's Personal Health Information Protection Act, PHIPA)* which sets out the ground rules for how organizations may collect, use and disclose personal information.

We will inform our clients and customers why and how we collect, use and disclose their personal information, obtain their consent where required, and handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Personal Information Protection Policy, in compliance with PIPEDA and PHIPHA, outlines the principles and practices we will follow in protecting clients' and customers' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our clients' and customers' personal information and allowing our clients' and customers' to request access to, and correction of, their personal information. We will only collect such information that is absolutely necessary to provide the required client/customer services.

**SCOPE OF THIS POLICY:** This Privacy Policy for personal Information protection applies to AlphaBee Employees. This policy also applies to any Associates charged with collecting, using or disclosing personal information on behalf of our organization.

This Privacy Policy has been developed to support the following ten principles related to Personal Information: Accountability; Purpose of Information Collection; Consent; Limit Collection & Use; Retention and Disclosure of Information; Accuracy of Information; Safeguarding Information; Openness to Individual Access & Challenging Compliance

## DEFINITIONS:

**Personal Information** –means information about an identifiable *individual* : e.g. personal information includes name, age, home address and phone number, social insurance number, marital status, religion, income, credit history, medical information, education, employment information.

Personal information **does not include** the name, title or business address or telephone number of an employee of an organization.

**Privacy Officer** – means the individual designated responsibility for ensuring that organization complies with this policy and legislated privacy laws.

**Consent:** Refers to voluntary agreement with what is being done or proposed. Consent can be either expressed or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

**Disclosure:** Making personal information available to others outside the organization.

**Use:** Refers to the treatment and handling of personal information within an organization or locations where services are provided on behalf of the organization.

**The Organization:** Throughout this policy the term "the organization" is taken to mean AlphaBee

### 1. ACCOUNTABILITY:

**1.1 The CEO/Designate:** is accountable for defining and approving the organization's Privacy Policy and for ensuring processes are put in place to support compliance throughout the organization. These processes include but are not limited to initial training of personnel during orientation, annual refresher communications, and updating of information as required to keep abreast of legislative compliance.

**1.2 All Employees:** are accountable for understanding and complying with the processes put in place to safeguard client/customer and for reporting any breaches as soon as they are identified. All employees are responsible for making suggestions for ongoing quality improvement of our processes. Organization employees are granted access to information they require to do their work and have different levels of access related to work requirements. All employees with access to client information are expected to comply with the Privacy Policy, to adhere to the *Privacy Act* and the ten principles as set out in the *Personal Health Information Protection Act* (PHIPA) and *Personal Information Protection and Electronic Documents Act* (PIPEDA). They declare their understanding and agree to abide by the policy by signing a Confidentiality Agreement as a condition of employment or employment contract agreement. The obligation to maintain confidentiality remains in effect even after termination of employment or relationship with the organization.

### 2. Collection of personal information:

2.1 The organization determines the purpose of collecting information before or at the time of information collection. The collection of personal client information is for the purpose of assessing the client's service needs during the intake process to ensure we can meet the requirements of the referral. Staff are trained to explain, upon client request why it is needed and how it will be used and disclosed in order to provide clients with the most appropriate services. Unless the purposes for collecting personal information are obvious and the client, customer, voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

2.2 We will only collect client/customer information that is necessary to fulfill the following purposes:

- the development of an effective plan of support to assist each client meet their identified goals in the location and at the time that best meets the client's needs
- the assignment of appropriate staff with the specialized training and availability to provide the required support
- All information regarding organization collection of personal client information is to be documented on approved forms which have been reviewed to ensure the information being requested is necessary to the provision of service. We commit to limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Assigned staff are trained regarding their duty to explain to a client the reason specific information is required in order to arrange the required service upon the client/caregiver's request. Examples include but are not limited to the following:
  - To verify identity and age appropriate activities, we collect name, home address, home telephone number and birth date;
  - To identify client, customer service preferences; we may ask about a range of options that the client would prefer and preferred options that would be available in a variety of settings and locations
  - To provide behavioural services; we would ask about situations that may cause anxiety, precede undesirable behaviours or encourage desirable outcomes.
  - Information to support health & safety e.g. emergency contact information, health considerations for support. Information that is necessary to meet regulatory requirements
  - quality improvement initiatives such as anonymous client and employee satisfaction surveys, expressed consent is sought and clients and employees are notified that their participation is voluntary.

2.3 All employees authorized to collect personal information as part of their duties, are responsible for ensuring they understand the reason such information is necessary to provide the requested services prior to collecting that information.

### **3. Obtaining Consent**

3.1 The personal information that is given to the organization in trust, will remain confidential, will not circulate outside of the agency in an unauthorized manner, and will not pass between employees for reasons other than for appropriate consultations.

3.2 The organization will inform the client or employee the purpose of the collection, use or disclosure of their personal information and will obtain the individual's consent before or at the time of collection, and when a new use of their information is identified. There are two types of consents used. The **inferred consent** where the individual complies with the request and provides the information requested, in this case the consent is **implied**. **Consent** will never be implied if an individual specifically states that their personal information may not be collected, used or disclosed. The second type is the **express consent** when the individual explicitly agrees to the collection, use and disclosure of their personal information which may be given in writing, verbally, by telephone or electronically. Express consent will be asked when disclosing personal information to a third party. If written consent cannot be obtained, a note in the client's file will indicate the time, date and that the verbal consent was received

3.3 Consent will be obtained through an appropriate substitute decision maker when the individual does not have the capacity to consent. Failure to consent will not result in services being withheld, unless the information is required to provide a specific service. The organization respects individuals' right to withdraw consent and will explain the implications, if any, to the client or employee.

3.4 In the case of an emergency, to prevent serious and imminent harm to themselves or others, the client's or employee's information will only be disclosed to the appropriate regulatory/professional body. In addition, if investigators appointed by the appropriate regulatory/professional body submit a written request to obtain personal records/information, the company will be legally obligated to make that information available to them. Such investigators must first furnish evidence of their appointment and the CEO/Privacy Officer/Designate will be notified immediately.

3.5 Providing Support subcontracted by a third party: In situations where Employees are providing subcontracted support in another facility on behalf of the organization, we will follow the protocol of the first party organization and notify their Privacy Officer as well.

#### **4. Limit Use, Disclosure and Retention**

4.1 The Organization will not use or disclose personal information for the purposes other than those for which it was collected, unless the individual consents otherwise, or is authorized or required by law. We use personal information for providing services, case discussions, consultations, treatments and reporting purposes to the facilities, funders or persons who have contracted agreements with the organization to provide support.

4.2 Except where required by law, client and employee information is never released without signed and dated consent, or that of the client's substitute decision maker. Personal information within The Organization is restricted to employees, administrative personnel, student placements who need access in order to provide services. When a provider refers a client to a service outside in order to maintain/provide appropriate level of consultation and/or supervision and continuity of care, certain client information may be required by that service provider. The consent is implied if the client agrees to the referral.

4.3 All client records shall be retained according to the policy pertaining to the records retention schedule of the organization. The physical records containing personal information will be destroyed,

erased or made anonymous in a secure manner in accordance with legislative and contract requirements related to the specific services provided.

## **5. Accuracy**

5.1 The Organization will assume that the personal information collected is accurate and complete since all the information comes directly from the individual and will ensure that opportunities exist for individuals to update their personal information on an ongoing basis.

## **6. Safeguard**

6.1 The Organization will take reasonable precautions to protect all personal information against loss, theft, defacement, tampering, unauthorized access, disclosure, copying or modification. The following security safeguards will be used to provide necessary protection:

- Physical measures (e.g., locked file cabinets and restricting access to offices)
- Technological measures (e.g., passwords and encryption);
- Agency measures (e.g., policies governing access to information and contract).
- Staff training and signed statements of understanding as outlined in relevant human resource policies.

6.2 In the case of breach, where the personal information is lost, stolen or accessed by unauthorized persons, the client will be notified as soon as possible by the Organization.

## **7. Openness**

7.1 The Organization's Privacy Policies and Procedures are openly communicated to all individuals through our website. All enquiries about the policies or personal information management are to be referred to the Privacy Officer.

## **8. Individual Access**

8.1 At any time, individuals can challenge the accuracy and completeness of their personal information at the Organization and may have it corrected or updated, if appropriate. In order to access personal information, a written form called "Request Access to Personal Service Record" will need to be filled out and sent to the Privacy Officer. Provided that the Organization is authorized to provide the information by law and that it will not result in harm to the individual or to another person, the individual will be given access to this information either directly or through an employee designated by the Privacy Officer within 30 days of receiving the request. The normal 30-day response time limit can be extended for a maximum of 30 additional days, according to specific criteria as follows:

- Responding to the request within the original 30 days would unreasonably interfere with activities of Organization
- Additional time is needed to conduct consultation, or is necessary to convert personal information to an alternate format.

8.2 The Organization will inform the individual seeking access to the information within 30 days of receiving the request, if it requires an extension. As well, the Organization will inform the individual of his or her right to submit a complaint to the Ontario Privacy Commissioner's Office.

## **9. Challenging Compliance**

9.1 All enquiries about the Organization's compliance to the ten principles are to be directed to the Privacy Officer. The Organization will inform individuals who make inquiries or submit complaints about the complaint procedures. The Privacy Officer/Designate will investigate all complaints and breach of information. The Organization will take appropriate measures to ensure information handling practices and procedures are adhered to and will take appropriate measures, including, if necessary, amending our policies and practices.

We take Privacy of Information very seriously. We understand that clients give us their personal information in trust that it will be kept confidential.

## **10. Service Provided to a Third Party**

10.1 In cases where the Organization holds a contract to provide support services to another entity (facility, hospital, school) the Organization understands that personal information belongs to the agency who has subcontracted our services. The Organization commits to abide by the Privacy Policy of that facility and to maintain any records, audits, information shared as part of the service requirement as outlined in applicable service agreements.

10.2 In cases where the organization receives queries or complaints about the handling of personal information for services provided as part of a service agreement to a third party, the client will be directed to the Privacy Officer of the Third Party. The Privacy Officer of our organization will be informed of the situation.

## **Records & Documentation**

- Client Intake Forms
- Client Electronic Record
- Employee signed Confidentiality Agreement
- Contract Agreements with Third Parties

## **References & Resources**

Office of the Privacy Commissioner of Canada  
[http://www.priv.gc.ca/search-recherche/index\\_e.asp](http://www.priv.gc.ca/search-recherche/index_e.asp)