EMPLOYEE AND STAFF INFORMATION GUIDE TO COMPANY PRIVACY POLICY

As an employee or associate of WM+A, AlphaBee and Interim, you will have access to personal information about the clients you support. This information will include obvious requirements such as name, address, contact information, location of service to be delivered; it may also include sensitive details of challenging behaviours and events that precede or follow situations and health issues that may have impact on how situations can be handled. The Organization commits to only collecting the type and amount of information from our clients that you will need to assist them meet the objectives in their support plans.

It is imperative that you know and understand your responsibilities for safe guarding sensitive personal information. Safeguarding the client personal information that has been entrusted to you in order to carry out the objectives of the client's service plan is a legal requirement under the privacy laws defined by Acts pronounced by national and provincial ministries . Two of the main Acts with which you must comply are *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.

The Acts in Brief

Organizations covered by privacy laws must **obtain an individual's consent** when they **collect, use or disclose** the individual's personal information. The individual has a right to **access** personal information held by the organization and to challenge its **accuracy**, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, **consent must be obtained again**. Individuals should also be assured that their information will be protected by specific **safeguards**, including measures such as **locked cabinets, computer passwords or encryption.**

Complaints

An individual may complain to the organization in question or to the Office of the Privacy Commissioner of Canada about any alleged breaches of the law. The Commissioner may also initiate a complaint, if there are reasonable grounds.

Offences

It is an offence to:

- destroy personal information that an individual has requested;
- retaliate against an employee who has complained to the Commissioner
- obstruct a complaint investigation or an audit by the Commissioner or her delegate.

Important Information You Need To Know

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.

Collection of Personal Information - Collection of Personal Information is generally undertaken during the referral process by authorized personnel. Intake forms have been created to compile the information needed to provide the required services. If more information is required during the course of service, it must be documented with appropriate justification and client consent. If you are authorized to collect information, it is imperative you understand the reasons why this information is required and that you are able to explain the reason to a client or substitute decision maker. All client information must be kept in authorized locations. Most information is stored in Oaiis where it is protected by encryption and firewalls and made available with password protection for multiple levels of access only to those who need to know. Hard copies of information must be stored securely in locked cabinets where it is protected from theft, fire and water damage. IF you are transporting client information, it must be kept in an appropriate bag or case, under your control at all times. Client information should not be left in the main body of a car or in a car trunk overnight.

Accountability of organization : Dunya Marijan, **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. Dunya may appoint a Designate when she is unavailable to address a situation that cannot be delayed and she may delegate to others some of the responsibilities for which she is accountable.

Accountability of staff: 1. You need to know that when you are approached internally or externally about privacy concerns, complaints from the public or requests for correction, you need to direct the person to the Privacy Officer unless you have been clearly authorized to speak on behalf of the organization. ***2.*** Before you ask a client for private information, you need to be able to explain why you are asking for that information and how it will be used. ***3.*** If you need to share that information with an external party e.g. case conference, you should check with the privacy officer to see if a written client's consent will be required. ***4.*** When handling client information, you must take all precautions to prevent it from becoming lost, defaced, or left in view of those who do not need to know that information. ***5.*** When discussing a specific client's support with another team member, be sure to do this in a private place where the conversation cannot be overheard by others who are not part of that client's support team. ***6.*** If you have concerns about how we collect or handle information, share these concerns or ideas for improvement with the Privacy Officer so that we can make quality improvements. ***7.*** If you have been assigned to provide supports to clients in another facility (e.g. hospital, school), clients and their records are considered the responsibility of that facility. Your role in this case is to follow the privacy procedures in that organization. When in doubt, consult with our own Privacy Officer. **8.** Clients may give us signed consent for some aspect of service. They may decide to withdraw that consent. You should be able to explain what may happen if they withdraw that consent so that they are not uninformed of any consequences to their service.

Informing our clients: The organization has prepared a statement written in clear language to inform clients of their rights under the privacy laws of Canada and Ontario and how to ensure we respect those rights. A

copy is posted in each office facility, there is a link on the website and we will include this information in future client brochures. It would be good practice to review that communication for your own understanding. If our clients have difficulty in reading and understanding this information, it is our role to find a way to present the information in terms they can understand. E.g. if a client is blind, you could read it to them or make an audio tape available.

Training our staff in privacy laws: This guideline and our Privacy Policy P-10 have been developed to assist our staff in understanding the privacy laws and their responsibilities and the organization's responsibilities under the various Acts (PIPEDA, PHIFA). This material will form a key module in staff orientation and refresher communications will be disseminated on privacy to reinforce understanding and awareness. All staff (employees and Associates are required to complete privacy quizzes that may be administered from time to time and also to sign off Agreements to Comply as a condition of contract or employment agreements. All staff will be informed of any changes to privacy laws or issues that may be raised because of technological changes, internal reviews and audits, public complaints and decisions of the courts.

Information for Employees and customers: Our Privacy Policy has been developed to outline how our organization complies with relevant privacy legislation. This policy is available via website link and sets out how we obtain personal information, the process for making an inquiry or complaint, what information is collected by our organization and how it is used, and under what circumstances it would be made available to a third party. It also sets out our desire to limit the collection of information to what is required to provide the required service. The policy clearly defines how we will carry out our responsibilities related to the ten principles of collecting, using, sharing, handling, obtaining consents, making information accessible, investigating complaint

Third Party Transfers: When a client has provided consent to transfer information to a third party, we ensure this is arranged according to a contract arrangement which limits the third party's use of information to purposes necessary to fulfill the contract. When a Third Party contracts with us to provide services to their clients, we sign a service agreement regarding access to information, handling complaints, disposal or return of information we receive.

Ensuring Accuracy of Information: When receiving information from a client, we review the information with the client to ensure we have transcribed key information accurately. Clients are requested to advise of any changes over time to the information provided so that their care continues to meet their requirements.

Safeguards: To the greatest extent possible, key information is stored electronically and significant investment has been made so that our system ensures that information is encrypted, has multiple layers of accessibility depending on need to know, and backup systems are effective to prevent loss, deletion of entries, read and write options, etc. Staff are directed to protect personal information and not leave it displayed on screens or desktops in their absence. They are directed to properly identify individuals and substitute decision makers before disclosing information about a client. Only authorized staff may add, change, delete information in the system. User accounts, access rights and security authorizations are part of our records management system.

Requests to access to personal information: When there is a request from a client to view their personal information, staff are directed to consult with the Privacy Officer. We need to ensure that the record does not inadvertently disclose information about another party that would be a breach of their information. While

personal information is generally easily accessed as required and our systems facilitate the retrieval and accurate reporting of an individual's information, including disclosures to third party organizations, we need to ensure no other person's information is breached. We have informed our clients of the time limits allowed by the law to respond to access requests, but in practice we are able to respond relatively quickly. Information is provided at minimal or no cost. Preparing information in response to a legal request, may take longer depending on complicating circumstances and we would inform the requester in advance of any costs involved. We make every effort to provide information in formats understandable to the requestor. E.g. presently our system would not produce the information in Braille but we would offer to read the information to the requestor or arrange to have it processed in Braille for a fee.

Handling Complaints: We welcome the opportunity to address complaints and these are addressed as quickly as possible. We make every effort to settle the complaint in a manner that is acceptable to the client. If we are unable to achieve a resolution that is mutually agreeable, we would assist the complainant to find another avenue e.g. provide information on contacting the Provincial Privacy Commissioner. We review our complaints for trends and use that information for quality improvements to our systems. We bring complaints to the attention of staff involved as appropriate to share how we addressed the issue and what changes need to be made if any to prevent it from happening again.

Privacy Officer: This role is accountable for the following organizational functions: **1.** Reviewing privacy practices in all programs of the organization **2.** Overseeing training of all employees/associates to ensure they understand the privacy laws and implications for their work **3.** Ensuring all employees/associates are kept up to date on new developments in privacy issues and best practice **4.** Handling of Complaints: investigate and determine actions to address and resolve matters within timelines outlined in the Privacy Policy. **5.** Mentoring designates to carry out functions within the role at her discretion. **6.** In unusual circumstances acting as custodian of private information at a client's request to be used only as instructed by the Client. **7.** Explain to the public the steps and procedures for requesting Personal Information and Filing Complaints. This role is further detailed in **Job Description: Privacy Officer**

When you have completed reading this handout and the applicable documents (Privacy Policy P-10 and the Client Commitment Information Sheet) we welcome your feedback on other areas that you feel should be clarified with more detail. As we continue to improve our package on this topic, we will be making revisions and additions to make as easy as possible to support the understanding of everyone who collects or is provided with personal information under this legislation.

We welcome your feedback.