PRIVACY POLICY

Privacy of Personal Information Policy

Approved by the Board of Directors:

Accommodation, Information and Support, Inc. (AIS) collects personal information, including personal health information, about its clients during the application process and throughout the duration of the tenancy.

AIS must comply with all applicable privacy legislation, including but not limited to the Personal Health Information Protection Act (PHIPA) which sets standards for the collection, use, disclosure and safeguarding of personal health information and the individuals' rights of access to and correction of records of their own information.

Privacy Officer

The AIS Executive Director acts as the Privacy Officer for AIS, and is responsible for the organization's compliance with all privacy legislation.

The Privacy Officer's duties are to:

review AIS's policies and practices with regard to personal information

1. implement any necessary changes to promote compliance with AIS's policy regarding the collection, use and disclosure of personal information
2. inform clients and the public on how AIS treats personal information
3. respond to questions and respond to complaints about privacy issues from clients and/or the public act as a resource to AIS staff on privacy issues

Definition of Personal Information

For the purpose of this policy, personal information means:

1. identifiable information about an individual, including any information that could identify the individual if it were linked to other personal health information, including about an individual's physical or mental health
2. Any identifying number assigned to an individual which could lead to their identification (e.g. health card (OHIP) number)
3. Information about an individual's income and/or assets

4. Bank account and credit card information
5. Information about rent payment history

Personal information does NOT include statistical data which is summarized in such a way as to not identify any individuals.

Business contact information and certain publicly-available information such as name, address and telephone number (as published in telephone directories) is not considered personal information.

Collection of Information

AIS will collect personal information only for the following purposes:

1. to approve tenancy and determine appropriate unit type and size
2. to determine income and assets for rent calculation
3. to demonstrate compliance with funding requirements
4. to protect and promote the health and safety of clients
5. to ascertain service levels required in supportive housing

Staff must not seek out personal information about clients or applicants unless it is required to fulfil the purposes above and to their duties at AIS.

All publicly available documents used for collection of personal information shall state:

a) the purpose(s) of the collection;
b) contact information for the Privacy Officer who can answer questions and respond to complaints about the collection, use or disclosure of the information;

AIS will require tenants to sign an agreement with AIS outlining the types of service available to the clients and the responsibilities of the AIS.

Protection of Information

- All staff, board members, volunteers and students on placement will be required to sign a confidentiality agreement.
- Applicant and client information (including information on databases) must be safeguarded against theft, loss and unauthorized access or disclosure.
- Applicant/client information must be stored in a locked filing cabinet. Secure storage facilities must be provided for archived applicant/client and accounting information.
- Staff should have access to records containing personal information on a "need to know" basis, only if required in order to fulfil their duties at AIS.

- When communicating client issues to the Board, staff should use non-identifying information as much as possible. For example, arrears report should use codes in place of the actual names.
- All staff have a responsibility to ensure that unauthorized individuals do not have unsupervised access to areas where files containing personal information are kept and used.
- Personal information will be disposed of at the end of the required storage period for client records of 7 years after the client has moved out, and for financial records of 7 years after the end of the fiscal year.
- Paper-based personal information must be shredded prior to disposal. Electronic media must be purged prior to disposal.

Release of Information

- Unless permitted or required by law, no personal information will be released to third parties without the written consent of the individual.
- It is not necessary to have a signed consent to release information where the disclosure is permitted or required by law, for example, to collect a debt using a collection agency, or for an Ontario Rental Housing Tribunal or Small Claims action or other legal proceeding.
- When responding to inquiries for references, staff must first obtain the client's consent and should limit information provided to the questioner, e.g. confirming only the information already provided by the individual making the inquiry.
- Staff will take reasonable care to confirm the identity of the people to whom information is released.

Personal information may be released to the following:

1. Funders and Auditor: AIS, in order to be in compliance with funding program requirements, must release information to funders and auditors. People doing these jobs have their own professional code of ethics and are required to maintain confidentiality. Staff should confirm that the person concerned is seeking access legitimately.
2. Researchers: AIS may be asked to assist a researcher who may be from an academic institution or who may be independent. The Executive Director must approve all such requests for personal information. Personal health information would only be released if the researcher complies with the research rules under PHIPA, including having the research project reviewed and approved by a research ethics board.
3. Law Enforcement: While AIS has a responsibility to protect the rights of applicants and clients to privacy, this responsibility must be balanced with an obligation to the broader community. Law enforcement agencies requesting personal information about applicants or current tenants will be required to provide a written legal document called a "warrant" before information will be released.

Personal information may be released to the police in circumstances which include, but are not limited to:

i. Staff with personal knowledge may choose to report criminal activity, including theft, damage, fraud, illegal drugs or other illegal activity in a building.
ii. With respect to crimes against persons, witnesses may choose to report and provide appropriate information to the police so that charges can be laid. Staff may also offer to assist a client who wishes to make such a report.
iii. Generally, victims of crimes are responsible for reporting the crime directly to the police.
iv. However, if the victim is a child where abuse is suspected, the law requires a report to Children's Aid Society. This duty to report is required under the Child and Family Services Act, Section 72.
v. AIS will also consider whether in specific cases, a report to police would be appropriate where a person suffers from a disability that renders them incapable of making the decision to report.
vi. Health and Safety Officials: Information will be provided where required to protect that health and safety of the individual or a third party, such as mandatory reporting to public health in limited circumstances.
vii. Emergency Contacts: It may be appropriate to use personal information to contact a community service agency or a designated relative in exceptional circumstances, such as, when using an emergency contact provided by a client and held on file, or contacting medical support services when a client is unable to function and maintain his/her tenancy.

Access to and Correction of Personal Information

- The Privacy Officer will respond to all requests for access to or correction of personal information.
- An individual who provides satisfactory identification will be given access to that information, except in limited circumstances, including where to do so would jeopardize an ongoing law enforcement proceeding.
- The individual may make a request for expedited access.
- If the Privacy Officer believes that releasing personal information to an individual would pose a serious risk of harm to the mental or physical health or security of any person, including the individual to whom the information relates, he or she will not release the information. The individual will be told of the right to make a complaint to the Information and Privacy Commissioner about the refusal to grant access.
- An individual may request correction of his or her information, subject to certain exceptions. If the Privacy Officer is not in agreement with the individual's request for correction, the individual may attach a statement of disagreement to the information.
- The Privacy Officer will make as much of the record available as possible, even if some parts of it are withheld. The Privacy Officer will prepare responses to all requests for access and correction.

Procedure for Handling Complaints

The Privacy Officer will respond to all complaints about collection, use, disclosure, storage and disposal of personal information within thirty days of the request being made, and advise the complainant as to the action that has been taken. If a particular request is very complex or requires extensive searching or consultation with others, that timeframe may be extended by an additional thirty days, on notice to the individual as soon as possible within the first thirty days.

Each complaint will be assessed to determine whether:

- Information was collected, used, released or disposed of inappropriately.
- AIS's policies and procedures need to be strengthened.
- Disciplinary or other action needs to be taken with respect to a breach of the AIS privacy policy or a confidentiality agreement.

Where necessary, the Privacy Officer will make the necessary recommendations to the Executive Director in connection with resolution of the complaint.

Breach of Confidentiality

A breach of confidentiality includes:

- Discussion of any confidential information within or outside the organization specifically with, or where it may be heard by, individuals who are not authorized to receive that information.
- Providing confidential information or records to unauthorized individuals.
- Leaving confidential information in written form or displayed on a computer terminal in a location where it may be viewed by unauthorized individuals.

A breach of confidentiality may be grounds for staff to be disciplined or terminated.