



Section: 02 ORGANIZATIONAL PLANNING AND PERFORMANCE	Date Issued: May 2017 Supersedes Policy: November 2015	Page: 1 of 4
Subject: 2.10 PRIVACY AND CONFIDENTIALITY		

Policy

Anago's privacy and confidentiality policy guides the collection, use and release of personal information to comply with provincial and federal privacy legislation to ensure responsible and transparent practices in the management of personal information.

Procedure

Information will be used only for the purpose it is intended and is limited to the use of personal information to the purposes for which the information was provided.

Anago's Executive Director is appointed as the Privacy Officer who ensures the following principles are embraced:

- 1) **Accountability:** Anago is responsible for personal information in its care, custody and/or control. To this end, Anago is committed to educate its employees on their responsibilities. The Privacy Officer ensures that the collections and storage of personal information is treated in a manner that is respectful of the individual and ensures the confidentiality of individual and employee files, by monitoring access, and for investigating, documenting and appropriately managing all violations of this Policy.
- 2) **Identifying Purpose:** Unless the purpose is self-evident, Anago shall clearly explain to the individual(s) identified the purpose for which information is collected before or at the time of collection.
- 3) **Consent:** Anago shall ensure the informed consent of individuals served is obtained for the collection, use and release of their personal information, except where permitted or required by law. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative, such as a substitute decision maker. Express consent can be given orally, electronically, or in writing, but it is always unequivocal and does not require any inference on the part of Anago. Implied consent is consent that can reasonably be inferred from an individual's action or inaction. Anago shall also ensure that individuals understand the implications of not providing their consent, and what notice would be required if consent is withdrawn at any point.
- 4) **Limiting Collection:** Anago shall collect personal information only by fair and lawful means limiting the collection of personal information to only those details necessary for the purpose(s) expressed.
- 5) **Limiting Use, Disclosure and Retention:** Personal information shall only be used for the purpose(s) for which it was collected unless additional consent has been obtained or when it is required or permitted by law. It will be retained only as long as necessary for these purposes or as required by law.



Section: 02 ORGANIZATIONAL PLANNING AND PERFORMANCE	Date Issued: May 2017 Supersedes Policy: November 2015	Page: 2 of 4
Subject: 2.10 PRIVACY AND CONFIDENTIALITY		

- 6) **Accuracy:** Personal information shall be maintained in as accurate, complete and current form as is necessary to fulfill the purposes for which it was collected.
- 7) **Safeguarding:** Personal information is collected by physical, procedural and electronic security safeguards appropriate to the type of information collected.
- 8) **Openness:** Anago shall make information available to individuals concerning the policies and practices that apply to the management of their information.
- 9) **Access:** Upon request, Anago shall inform an individual of the existence, use and disclosure of personal information. Individuals may at any time verify the accuracy and completeness of the information and request that it be amended if appropriate.
- 10) **Challenging Compliance:** Anago has identified the Executive Director to serve as the contact point for all questions by both internal (i.e. employee) and external individuals with respect to these principles. To this end, a written statement is made available on Anago's website regarding the procedure for making a complaint in regards to a breach of privacy. All inquiries shall be directed to:

Privacy Officer
Anago
371 Princess Avenue
London ON N6B 2A7
(519) 435-1099 X 102

Additionally, the Privacy Officer shall:

- 1) Review the policies and practices with regard to personal information.
- 2) Implement the necessary changes to guarantee that the collection and retrieval of personal information follows relevant legislation.
- 3) Work with Human Resources to communicate information to relevant parties as to how personal information is collected, used and disclosed.
- 4) Respond to requests for access to or correction of personal information. An individual will be able to challenge the accuracy and completeness of the information and have it amended, as appropriate. The individual will not have access to third party information.
- 5) Review all complaints with regard to breach and/or perceived breach of privacy.
- 6) Evaluate understanding and compliance during internal audits.



Section: 02 ORGANIZATIONAL PLANNING AND PERFORMANCE	Date Issued: May 2017 Supersedes Policy: November 2015	Page: 3 of 4
Subject: 2.10 PRIVACY AND CONFIDENTIALITY		

7) Initiate improvement initiatives as a result of complaints.

Training

The Manager is responsible for reviewing privacy and confidentiality with employees at the time of hire and ensure they sign a Privacy and Confidentiality Statement (HR 109) which shall be retained in their employee file. The Manager will involve employees in discussion of examples and scenarios that are frequently encountered in their specific roles.

To prevent unauthorized access to personal information, Anago data is stored centrally and securely accessed remotely by a secure, VPN-based, WAN. Servers and related data are imaged daily and archived to portable USB drives. Electronic storage is for Agency-related data only and storage of personal data is expressly prohibited. No electronic Anago data shall be stored on computer hard drives, or portable. Electronic documents and databases containing confidential files with personal information are password protected. The Directors shall ensure all Anago computers at their sites are secured to ensure the integrity of the data and functionality of the closed system. Additionally;

- All employees and Board members are required to sign the Privacy and Confidentiality Statement (HR 109).
- Applicants, individuals receiving services and employee information are stored in a locked filing cabinet. Secure storage facilities are provided for archived applicant/client/employee and accounting information.
- Employees and members of the Board, where appropriate, have access to records containing personal information, only if required in order to fulfill their duties.
- When communicating individuals receiving services or employee issues to the Board, employees use non-identifying information as much as possible. For example, reports shall use initials in place of the actual names.
- Telephones equipped with voice mail are password protected against unauthorized access.
- Visitors do not have unsupervised access to areas where files are kept and used
- Paper-based personal information is shredded to denote proper disposal and is handled in a secure fashion.

No personal information is released to third parties without the written consent of the employee through the completion of Release of Information (HR 200) (i.e. credit references, personal references, etc.). Anago employees take reasonable care to confirm the identity of the individual to whom information is released.

Improper Disclosure

In the event of any improper disclosure or unauthorized access to personal information, Anago employees and/or contractor(s) must promptly advise the Privacy Officer. The Privacy Officer shall evaluate the incident and refer the matter to the appropriate individual(s) for corrective measures as



POLICY AND PROCEDURE MANUAL

Section: 02 ORGANIZATIONAL PLANNING AND PERFORMANCE	Date Issued: May 2017 Supersedes Policy: November 2015	Page: 4 of 4
Subject: 2.10 PRIVACY AND CONFIDENTIALITY		

required. In the event of a confidentiality breach, the Privacy Officer will notify employees or individuals who are impacted by the case of theft, loss, or unauthorized use or release of their personal information.

Responsibility

All employees, students, volunteers and third party (individuals/organizations) are responsible for complying with the intent and principles of this Policy with respect to personal information to which they have access. Annually, employees review and sign the Code of Ethical Conduct, Privacy and Confidentiality Attestation and Offence Declaration (HR 221).

Reference: *Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA)*

Authorized by:

A handwritten signature in blue ink, appearing to be "K. G. ...", written over a horizontal line. Below the line, the text "Executive Director" is printed.

Executive Director

Date: May 2017