STATEMENT of POLICY and PROCEDURE			
Chapter:	Human Resources	Policy No.	**HR 4.07**
Section:	Employee Relations	Issued:	June 6, 2012
Subject:	**PERSONAL INFORMATION PROTECTION**	Effective:	June 6, 2012
Issue to:	All Manual Holders	Page:	1 of 6
		Revised:	**Annually Dec 11, 2024**
Issued by:	Board of Directors	Dated:	

1 POLICY

1.01 Glengarry Inter-Agency Group Inc. (GIAG) is committed to protecting the privacy of its employees, clients/customers and confidential business information.

1.02 Employees are obligated to ensure that personal information to which they may have access remains confidential, is only used for the purposes for which it was collected, and is not disclosed without authorization or used for personal gain.

1.03 Employees are required to read, agree to and sign a Declaration of Confidentiality.

1.04 Employees are required to follow all procedures regarding collection, use, and disclosure of personal information as set out in this policy.

1.05 Employees who disclose personal information contrary to this policy will be subject to disciplinary measures, up to and including discharge for cause.

1.06 The Executive Director is accountable for the implementation of this policy. Any issues or questions regarding this policy should be directed to the Executive Director.

2 PURPOSE

2.01 All employees at one time or another may receive personal, privileged and/or confidential information which may concern other employees, Agency operations or clients/customers. The purpose of this policy is to preserve the privacy of employees, clients and GIAG, by outlining obligations and procedures for dealing with personal, privileged and/or confidential information.

3 SCOPE

3.01 This policy applies to all employees, members of Board of Directors, volunteers, contractors, subcontractors of GIAG or anyone else who is granted access to personal, privileged and/or confidential information.

4 RESPONSIBILITY

4.01 Employees are responsible for:

- Keeping their own employee files current regarding name, address, phone number, dependents, etc.;

- Being familiar with and following policies and procedures regarding personal information;
- Obtaining the proper consents and authorizations prior to disclosure of personal, privileged and/or confidential information;
- Immediately reporting any breaches of confidentiality to their manager;
- Keeping private passwords and access to personal, privileged and/or confidential data;
- Explaining this policy to clients and referring them to the executive director if necessary;
- Relinquishing any personal, privileged, confidential or client information in their possession before or immediately upon termination of employment.

4.02 Managers are responsible for:

- Obtaining consent to the collection and use of personal information from employees;
- Ensuring policies and procedures regarding collection, use and disclosure of information of personal information are consistently adhered to;
- Obtaining the proper consents and authorizations prior to disclosure of information contained in employee records;
- Responding to requests for disclosure;
- Maintaining systems and procedures to ensure employee records are kept private;
- Responding to employees' requests for access to their files;
- Ensuring proper disposal of unnecessary files/information;
- Maintaining separate files to ensure that personal health information is protected;
- Cooperating with the executive director to investigate complaints or breaches of policy;
- Obtaining from terminating employees, prior to their termination, any personal, privileged, confidential or client information in their possession;
- Ensuring that disclosure of personal information or personal health information to a third party is done with the approval of the executive director in order to minimize risk of non-compliance with applicable legislative or regulatory regimes.

4.03 The Executive Director is responsible for:

- Internal compliance with applicable policies or legislation;
- Cooperating with managers, human resources and/or payroll personnel in developing internal policies for the collection, use and disclosure of personal information and personal health information of employees and clients;

- Monitoring and responding to third party requests for personal information or personal health information;
- Ensuring appropriate consents are obtained for the collection, use and disclosure of personal information and personal health information;
- Where collection, use or disclosure is permitted without prior consent, notifying individuals of the collection, use and disclosure of personal information and/or personal health information after such occurrence.

5 DEFINITIONS

5.01 "**Personal information**" is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title, business contact information or job description.

5.02 **"Personal health information"** is information about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision-makers on behalf of the individual.

5.03 "**Third parties**" are individuals or organizations other than the subject of the records or representatives of GIAG. Note that in certain circumstances, the Agency may be entitled to provide personal information to an external party acting as an agent of GIAG.

6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

6.01 *Personal Information Protection and Electronic Documents Act* (PIPEDA)

HR 4.08 — E-mail and Internet Use

7 PROCEDURE

7.01 Employee Records

(a) An employee's Manager, higher level managers, human resources and payroll personnel shall have access to employee records containing personal information. An employee's Manager, higher level managers, human resources and payroll personnel will have access to an employee's personal health information if the Executive Director determines that such access is permissible and necessary. Personal information and personal health information will not be disclosed outside of the organization without the knowledge and/or approval of the employee. Notwithstanding the foregoing, GIAG will cooperate with law enforcement agencies and will comply with any court order or law requiring disclosure of personal information without the employee's consent;

(b) Employees may request access to review their own file by making arrangements with the Payroll department. Employees shall provide at least twenty-four (24) hours notice to the Payroll department. Employees may obtain a copy of any document in their file which they have signed previously. No material contained in an employee file may be removed from the file. A representative of the Payroll department will be present during viewing of the file;

(c) An employee may provide a written notice of correction related to any data contained in the employee's file. The notice of correction shall be provided to the Payroll department;

(d) Employee requests for disclosure of their own personal information to third parties must be accompanied by a completed, signed and dated Authorization to Release Information form. This form should also be used in dealings with insurance companies with respect to employee benefits and to provide confirmation of earnings to financial institutions for lending purposes;

(e) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.

7.02 Client Information

Personal, privileged and/or confidential information about customers and clients may only be collected, used, disclosed and retained for the purposes identified by GIAG as necessary;

(a) Employees must ensure that no personal, privileged and/or confidential client information is disclosed without the client's consent and then only if security procedures are satisfied;

(b) Client information is only to be accessed by employees with appropriate authorization;

(c) Unless retention of personal information is specified by law for certain time periods,

personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.

7.03 Notwithstanding paragraphs 7.01(e) and 7.02(d), personal information that is the subject of a request by an individual or a Privacy Commission shall be retained as long as necessary to allow individuals to exhaust any recourse they may have under PIPEDA.

7.04 Concerns or complaints related to privacy issues must be made in writing to the Executive Director, setting out the details of the concern or complaint. The Executive Director shall investigate the matter forthwith and make a determination related the resolution of the concern(s) or complaint(s).

7.05 No employee shall be disadvantaged or denied any benefit of employment by reason that GIAG believes that an employee will do anything referred to paragraphs (a), (b), or (c) below, or by reason that an employee, acting in good faith and on the basis of reasonable belief:

(a) Has disclosed to the Privacy Commissioner of Canada that GIAG or any other person has contravened or intends to contravene a provision of PIPEDA related to the protection of personal information;

(b) Has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA related to the protection of personal information;

(c) Has done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA related to the protection of personal information not be contravened.

7.06 An employee who is found to be in breach of this policy will be subject to discipline up to and including discharge for cause.

7.07 **Electronic Platforms**

Even though GIAG provides third party resources and websites, GIAG does not have control over the content that is found on other websites and links that direct users away from its websites. GIAG is not responsible for the use of personal information outside its services.

Cookies are information stored on the hard drive of users computers that allow websites to recognize who it is accessing the website but the cookies on GIAG websites do not provide any private information such as email addresses or information on the users' identity.

Registration information is protected through the use of Secure Sockets Layer (SSL) software and the information that users provide to GIAG is encrypted.

GIAG's websites may contain links to other websites. GIAG is not responsible for the information shared with external websites or services provided by external websites.

8 ATTACHMENT

Declaration of Confidentiality Form
Authorization to Release Information Form