1. Privacy Officer

Name: Michele Petrasso

Role: Privacy Officer

Responsibilities:

- Overseeing compliance with PIPEDA and applicable laws

- Approving internal privacy procedures

- Responding to access requests and complaints

- Training staff and contractors

- Completing periodic privacy reviews

2. The 10 Fair Information Principles

1. Accountability

The Privacy Officer ensures all personal information is handled lawfully. Staff and contractors must follow this program. All investigations must be documented and reviewed for lawful purpose and proportionality.

2. Identifying Purposes

Before collecting personal information, the agency identifies and documents the purpose. Examples include insurance investigations, skip tracing, process serving, and personal relationship matters limited to public observations.

3. Consent

Consent is obtained whenever required. For investigations where consent cannot be obtained, the Privacy Officer determines whether a PIPEDA exception applies. When no exception applies, only publicly observable information is collected.

4. Limiting Collection

The agency collects only what is necessary. Intrusive methods are prohibited unless clearly lawful and proportionate. Personal matters are limited to public observations and basic behavioral information.

5. Limiting Use, Disclosure and Retention

Information is used only for its stated purpose. Disclosure is limited to clients, legal representatives, or as required by law. Files are retained for a defined period and then securely destroyed.

6. Accuracy

Information is recorded accurately, supported by evidence when possible. Surveillance logs and reports are factual and timestamped. Corrections or clarifications are documented.

7. Safeguards

Safeguards include encrypted storage, password-protected devices, limited access, and secure transfer of reports. Contractors sign confidentiality agreements. Personal devices are not used for investigative data.

8. Openness

This program is available to clients upon request. The agency explains how information is collected, stored, shared, and destroyed.

9. Individual Access

Individuals may request confirmation of whether the agency holds their information, access to it, or corrections. The Privacy Officer responds within 30 days unless an extension is permitted.

10. Challenging Compliance

Individuals may file privacy complaints with the Privacy Officer. Complaints are logged, investigated, and, if unresolved, may be taken to the Office of the Privacy Commissioner.

3. Internal Procedures

A. Intake Screening

All files are screened for lawful purpose, PIPEDA applicability, proportionality, and risks. Notes are documented.

B. Investigation Authorization

Each investigation requires written client agreement, confirmation of purpose, and privacy review notes.

C. Data Handling Rules

All data is stored on encrypted devices. Files use case numbers rather than full names. Transfers must be secure.

D. Surveillance Rules

Surveillance is limited to public places. No collection is made in areas with a reasonable expectation of privacy. Covert methods require documented justification.

E. Retention & Destruction

Files are stored for a set period and then securely destroyed by digital wiping, shredding, or removing cloud backups.

4. Training

Staff and contractors receive privacy orientation, annual refreshers, and case-specific guidance. Training is logged.

5. Third-Party Service Providers

Cloud services, data processors, and subcontractors must sign confidentiality agreements and follow equivalent safeguards. No personal information is stored outside Canada without approval.

6. Breach Response Plan

If a breach occurs:

1. Contain it immediately.

2. Notify the Privacy Officer.

3. Assess risk.

4. Notify affected individuals and OPC if required.

5. Document the breach.

6. Take steps to prevent recurrence.