Privacy Inquires and Privacy Complaints Policy

Department	Document Number	Organizational Scope	ICES Site	IPC Scope
PLO	PO.020	ICES Site-Specific Policy	ICES Network	All Acts
Original Date (Month yyyy)	**Last Review Date** (Month yyyy)	**Frequency of review**	**Next Review Due Date (Month yyyy)**	**Supersedes (if applicable)**
June 2014	September 2022	Triennially	September 2025	800PR-PR-003

Authority (Title)	Policy Owner (Title)
Chief Privacy & Legal Officer	Director, Privacy & Legal

Required Reviewers (Titles)		

Please refer to the **glossary** for terms and definitions.

1.0 PURPOSE

1.1 This **Policy** addresses how ICES manages **Privacy Complaints** and **Privacy Inquiries** from the public and relevant stakeholders.

2.0 SCOPE

2.1 This **Policy** applies to any **Privacy Complaint** or **Privacy Inquiry** received by **ICES Central** or an **ICES Site**.

2.2 A **Privacy Complaint** includes concerns or complaints relating to the privacy **Policies**, **Procedures**, and **Practices** implemented by ICES, and/or relating to the compliance of ICES with Ontario's *Personal Health Information Protection Act* **("PHIPA")**, the *Coroners Act*, and their applicable regulations.

2.3 A **Privacy Inquiry** includes inquiries relating to the privacy **Policies**, **Procedures,** and **Practices** implemented by ICES, and/or relating to the compliance of ICES with **PHIPA**, the *Coroners Act*, and their regulations.

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES **Chief Privacy and Legal Officer ("CPLO")**

3.2 approving and overseeing establishment of a process for responding to **Privacy Complaints** and **Privacy Inquiries**

3.3 ICES Privacy **Subject Matter Expert ("SME")**

3.4 managing and implementing the process for responding to **Privacy Complaints** and **Privacy Inquiries**

3.5 **ICES Employees, ICES Agents, Non-Appointed ICES Agents ("NAIAs"), Collaborating Researchers,** and **Third Party Researchers ("TPRs")**

3.6 Cooperating and assisting with the **Privacy Complaints** and **Privacy Inquiries** management process

4.0 DETAILS

4.1 Responsibility for managing **Privay Complaints** and **Privacy Inquiries**

4.1.1 The ICES **CPLO** is responsible for approving and overseeing establishment of a process for responding to **Privacy Complaints** and **Privacy Inquiries**. This process shall be designed to:

a. communicate to the public how and to whom to make **Privacy Complaints** and **Privacy Inquiries**;

b. receive **Privacy Complaints** and **Privacy Inquiries** from the public;

c. determine when to investigate **Privacy Complaints** and communicate the outcomes of those determinations to complainants;

d. create a process to investigate **Privacy Complaints**;

e. identify and remediate the causes of and factors contributing to **Privacy Complaints**;

f. track implementation of measures to remediate the causes of and factors contributing to **Privacy Complaints**;

g. inform complainants of investigation outcomes and resultant remediation measures;

h. notify third parties, where required, of **Privacy Complaints**;

i. respond to **Privacy Inquiries**; and

j. ensure documentation related to **Privacy Complaints** and **Privacy Inquiries** is created.

4.2 Gudiing principles for management for **Privacy Complaints** and **Privacy Inquiries**

4.2.1 ICES' management of **Privacy Complaints** and **Privacy Inquiries** is informed by the *Model Code for the Protection of Personal Information (CAN/CSA-Q830-96)*, having particular regard to the need to balance between accountability, openness and individual access, and safeguards.

4.3 Specific principles for management of **Privacy Complaints**

4.3.1 A **Privacy Complaint** will be investigated when it relates to ICES' functions as a **Prescribed Entity** under **PHIPA** and under the *Coroners Act,* and one of two of the following apply:

a. the **Privacy Complaint** provides reasonable grounds to believe that non-compliance with ICES' privacy **Policies**, **Procedures**, and **Practices**, **PHIPA**, and/or the *Coroners Act* has occurred or will occur—in other words, that there has been or there will be a **Privacy Incident** or **Privacy Breach**; or

b. the **Privacy Complaint** may indicate a deficiency in ICES' privacy **Policies**, **Procedures,** or **Practices**.

4.3.2 An investigation of a **Privacy Complaint** must follow the rules of procedural fairness, applied in a manner that is appropriate to the legal, institutional, and social context of the decision.

5.0 RELATED DOCUMENTATION

5.1 *Privacy and Security Incident Breach Management Policy*
5.2 *Discipline and Corrective Action in Relation to ICES Data Policy*
5.3 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*
5.4 *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy*
5.5 *Change Management Policy*

6.0 TRAINING AND COMMUNICATION

6.1 **Policies** and **Procedures** are available on the **ICES Intranet**.

6.2 This **Policy** and any administrative **Procedures** are communicated to all **ICES Agents** across the **ICES Network** during onboarding and on a yearly basis. **Policy** awareness is also supported and promoted by the **Policy Owner**.

6.3 Once new **Policies** are published to the **ICES Intranet**, they are communicated to **ICES Employees** in ICES OnTap, the weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 **ICES Agents** must comply with all applicable ICES **Policies** and **Procedures**.

7.2 **ICES Agents** must notify an ICES Privacy **Subject Matter Expert ("SME")** or ICES Security **SME** at the first reasonable opportunity if they breach or believe there has been a breach of ICES' privacy and security **Policies** or **Procedures**, in accordance with ICES' *Privacy and Security Incident Breach Management Policy* and associated **Procedures**, as set out in the framework posted on the ICES **PLO**/Cybersecurity site on the **ICES Intranet**.

7.3 All other violations under ICES privacy and security **Policies** and **Procedures** may be subject to a range of **Disciplinary Actions** including warning, temporary or permanent loss of **Access Privileges**, legal sanctions and/or termination of employment for cause, or contract with ICES pursuant to *ICES' Discipline and Corrective Action in Relation to ICES Data Policy* and ICES' *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy* and associated **Procedures**.

7.4 Compliance is subject to annual audit by an ICES Privacy **SME** or ICES Risk & Compliance Analyst pursuant to the **Annual Audit Schedule** established under ICES' *Privacy and Security Audit Policy*.

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this **Policy** must be in accordance with ICES' *Ongoing Review of Privacy and Security Policies, Procedures, Practices, and Exceptions Policy* and ICES' *Change Management Policy*.