Collingwood Psychotherapy & Yoga Centre

Cybersecurity & Data Breach Response Policy

1. Purpose

This policy outlines the proactive measures Collingwood Psychotherapy and Yoga Centre (CPYC) takes to protect digital information and the specific steps required should a data breach occur. This policy ensures compliance with the *Personal Health Information Protection Act* (PHIPA) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), while honoring our commitment to client privacy and relational integrity. Please refer to the CPYC Client Privacy, Confidentiality & Data Collection Policy.

2. Digital Protection Measures

To prevent unauthorized access to Personal Health Information (PHI), CPYC implements the following technical and administrative safeguards:

- **Platform Security:** We utilize "Jane" for client management, which is a PHIPA-compliant platform using bank-level encryption (SSL) to protect data in transit and at rest.
- **Access Control:** Access to client records is restricted to authorized personnel only (e.g., the primary therapist and essential administrative staff) on a "need-to-know" basis.
- **Device Security:** Any device used to access CPYC data (laptops, tablets, smartphones) must be encrypted and secured with a strong password, PIN, or biometric lock. Devices must never be left unattended while logged into client platforms.
- **Network Security:** Staff and contractors are prohibited from accessing PHI over unsecured public Wi-Fi networks. The use of a Virtual Private Network (VPN) or secure, password-protected private networks is required.
- **Password Hygiene:** All team members must use unique, complex passwords for CPYC-related accounts. Two-Factor Authentication (2FA) must be enabled on all platforms where available (e.g., Jane, Google Workspace).

3. Identifying a Data Breach

A data breach occurs when PHI is stolen, lost, or accessed by an unauthorized person. Examples include:

- A lost or stolen mobile device or laptop containing client information.
- A "phishing" email that results in unauthorized access to a CPYC email or Jane account.
- Accidentally sending a client's clinical notes or intake forms to the wrong recipient.
- Unauthorized "snooping" into files by staff or contractors without a clinical or administrative reason.

4. Data Breach Response Plan

In the event of a suspected or confirmed breach, CPYC follows the **"Contain, Assess, Notify"** protocol:

Step 1: Containment Immediately take steps to stop the breach and prevent further data loss. This may include:

- Changing passwords and enabling 2FA immediately.
- Remotely wiping a lost or stolen device.
- Contacting IT support or the software platform (e.g., Jane) to freeze account access.

Step 2: Assessment The Privacy Officer will investigate the breach to determine:

- The nature of the information involved.
- The number of individuals affected.
- The likelihood of "significant harm" (e.g., identity theft, bodily harm, or reputation damage).

Step 3: Notification

- **Affected Individuals:** CPYC will notify affected clients as soon as reasonably possible. We believe in "radical honesty"; we will explain what happened, what data was involved, and what we are doing to fix it.
- **Regulatory Bodies:** If the breach meets the threshold for "significant harm" or mandatory reporting under PHIPA, CPYC will notify the Information and Privacy Commissioner of Ontario (IPC).

Step 4: Prevention & Repair Following a breach, CPYC will conduct a "post-mortem" review to update security protocols, provide additional staff training, and ensure the vulnerability is closed.

5. Accountability

All therapists and contractors working with CPYC are responsible for adhering to these cybersecurity standards. Failure to follow security protocols (such as leaving a device unlocked or sharing passwords) is considered a violation of the CPYC Contractor Agreement.

6. Policy Review

This policy is reviewed annually to stay current with emerging digital threats and changes to Ontario privacy legislation.

Effective Date: January 15, 2026

Policy Owner: Privacy Officer: Office Manager (info@cpyc.ca)

Review Frequency: Annually

Next Review Date: January 2027

Status: Approved (V1)