PRIVACY BREACH POLICY

Approved By	Executive Management Team
Last Reviewed	November 14, 2017 (next review to be done within two years)
Responsible Role	Director, Communications, Marketing & Quality (Chief Privacy Officer)
Responsible Department	Marketing

PRIVACY BREACH POLICY

SECTION 1 – INTRODUCTION

1.1 Purpose

The purpose of this policy is to provide direction in the event of a privacy breach of the personal or confidential information of JVS Toronto clients or personnel, unless the personal information is collected, used or disclosed through the JVS Toronto website. This personal information is dealt with in the JVS Toronto Web Site Privacy Statement. See definition below.

This policy provides guidance on reasonable steps necessary to limit the breach, support an effective investigation and to assist with remediation.

1.2 Scope

The policy applies to all JVS Toronto employees, volunteers including Board and Board Committee members, placement students, contractors or consultants, and anyone working at or acting on behalf of JVS Toronto, and who are privy to personal information.

1.3 Definitions

Word/Term	Definition
Chief Privacy Officer	A member of the JVS Toronto executive management team who is appointed with the responsibility for managing the risks and business impacts of privacy laws and policies.
Confidentiality	The obligation of all JVS Toronto employees, or those acting on behalf of JVS Toronto, to keep personal information secret. Confidentiality arises in the course of a relationship in which private information is shared. As the sharing of personal information is essential for accurate assessment, diagnosis, provision of services and/or treatment of JVS Toronto clients, this ethical duty of confidentiality is imposed upon JVS Toronto to ensure that client information obtained in the course of providing services is kept secure and confidential.
Confidential Information	Refers to any information of a sensitive matter that should remain confidential.
Containment	Containment involves taking immediate corrective action to put an end to the unauthorized practice that lead to a privacy breach.
Disclosure	When personal or confidential information is shared.
Personnel	This refers to anyone working on behalf of JVS Toronto including full-time, part-time, casual and other employees, volunteers including Board and Board Committee members, placement students, contractors or consultants.
Personal Information	Section 2(1) of the *Personal Information Protection and Electronic Documents Act* (2000, c. 5) (PIPEDA) states that "personal information" means "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." For example, personal information may include performance reviews, doctor's notes, home address and a record of their sick days.
Privacy	The right of the individual to control the collection, use and disclosure of information about the individual, limiting it to that which is necessary. Privacy includes having the right to determine what information is collected, how it is used, and the ability to access collected information to review its security and accuracy. Privacy means having the right to choose the conditions and extent to which one's information is shared.

PRIVACY BREACH POLICY

Privacy Breach	An inappropriate access, use or disclosure of personal or confidential information including, without limitation: (1) unauthorized collection: collected coercively or without consent or for purposes not approved by JVS Toronto or the individual (2) unauthorized use: used for purposes not supported by JVS Toronto (3) unauthorized disclosure: disclosure without consent or legal authority, security breaches or loss of equipment containing personal information such as laptops or mobile device or loss of paper records or unauthorized or unsecured disposal of personal information (4) denial of client rights: such as collection, use or disclosure without consent, denial of access to personal information. Other breach examples include inappropriate access into client information (snooping), independently accessing one's own personal information or that of a colleague, members of management or other JVS Toronto personnel, family members, friends, acquaintances and people featured in the media.
Security	Preventing unauthorized access to personal or confidential information through physical, organizational or technological means. In other words, security is the measures taken to ensure the confidentiality, integrity and availability of personal information.
Third Party Service Providers	Contracted third parties used to carry out or manage programs or services on behalf of JVS Toronto and for the purposed of privacy breach reporting include all parties that receive personal or confidential information from JVS Toronto or collect personal information on behalf of JVS Toronto.

1.4. Related Policies

1.4.1 Privacy Policies

Business & Remote Office Privacy and Security Policy
Client Records Collection & Disclosure Policy
JVS Personnel Records Collection & Disclosure Policy
Privacy Breaches Policy
Privacy Complaint Resolution Policy
Records Retention & Destruction Policy

1.4.2 Additional Policies

Internet & Email Policy
Mobile Device Policy
Password Policy
Whistleblower Policy

1.5 Legislative Context

Child and Family Services Act
Ontario's Health Care Consent Act
Personal Health Information Protection Act, (PHIPA) 2004
Privacy and Personal Information Act (PIPA)
Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act
Social Work and Social Service Work Act
The Mental Health Act

PRIVACY BREACH POLICY

SECTION 2 - POLICY

2.1 Policy

It is JVS Toronto's policy to prevent privacy breaches by following a "culture of privacy" in adhering to all privacy protocols as detailed in JVS Toronto's privacy policies. Should a privacy breach occur through the loss, theft or unauthorized access of personal or confidential information of a JVS Toronto personnel or client, then the impact of the breach must be contained, and a prompt, reasonable, and coordinated response to the breach must be taken consistent with this policy.

NOTE: The following section, 3, "RESPONSIBILITY & PROCEDURE" represents best practices as determined by JVS Toronto, and is largely designed to provide guidance to designated JVS Toronto representatives. However, it is understood that, where appropriate, these representatives may adopt modified procedures in response to any given circumstance.

SECTION 3 – RESPONSIBILITY & PROCEDURE

3.1 Privacy Breach Prevention & Containment

3.1.1 JVS Toronto Personnel

Be alert to the potential for personal or confidential information to be compromised.

1. The Manager or Director should be notified immediately when JVS Toronto personnel become aware of a breach or suspected breach.
2. Where possible, the personnel will contain the suspected breach by suspending the process or activity that caused the breach or potential breach.

3.1.2 JVS Toronto Managers

Be alert to the potential for personal or confidential information to be compromised.

1. Where possible, contain the suspected breach by suspending or confirming suspension of the process or activity that caused the breach or potential breach.
2. Alert the Director of a breach or suspected breach and work with him/her to implement the five steps of the response protocol.
3. Inform the affected individuals, if required, and respond to questions or concerns.
4. Obtain all available information about the nature of the breach or suspected breach, and determine the events involved.
5. Ensure the details of the breach and corrective actions are documented using the **Privacy Breach Report Form**.

3.1.3 Director

1. Ensure that the five steps of the Privacy Breach Protocol are implemented.
2. Notify the Chief Privacy Officer and ensure that the situation is discussed with the Chief Privacy Officer prior to final resolution.
3. Support the JVS Toronto manager in responding to the breach.
4. Inform the Marketing Department.
5. Once the breach has been resolved, support the development of a prevention plan.
6. Make a report of findings and actions Chief Privacy Officer.

3.1.4 Marketing Department

1. Respond to questions from the public regarding the breach.

3.1.5 Chief Privacy Officer

1. Brief the Senior Management Team as necessary and appropriate.
2. Review the internal investigation reports and approve the recommended remedial action.
3. Monitor the implementation of the remedial action pertaining to privacy breaches.
4. Ensure that those whose personal information has been compromised are informed as required.
5. Escalate issues to the President & CEO when required.

3.1.6 Third-Party Service Providers

1. Take reasonable steps to monitor and enforce their compliance with the privacy requirements defined in the contract or service agreement and inform their JVS Toronto contact of all actual and suspected privacy breaches.
2. With support from the JVS Toronto contact, follow the steps outlined in **Section 3.2 Privacy Breach Policy.**

3.2 Privacy Breach Protocol

The following five steps will be initiated as soon as a privacy breach, or suspected breach, has been reported. The **Privacy Breach Report Form** will be used to document the breach and guide the manager through the breach management process.

3.2.1 Step 1 – Report and Assess

Report

Upon become aware of a possible breach of personal or confidential information, the suspected breach will be promptly reported to the Manager. This will occur even if the breach is suspected and not yet confirmed. The report will capture:

- What happened.
- Where it occurred.
- When the suspected incident occurred.
- How the potential breach was discovered.
- Where the information was breached eg: technology, paper files, verbally.
- Corrective action taken when the possible breach was discovered.

Assess

The Manager will assess the breach by asking the following questions:

Q1) Is personal or confidential information involved?

☐ yes ☐ no

Q2) Has unauthorized collection, use, disclosure or retention of personal or confidential information occurred?

☐ yes ☐ no

Q3) Has personal or confidential information been lost or stolen?

☐ yes ☐ no

If the answer is “Yes” to question 1, and “Yes” to either Questions 2 or 3, then it can be assumed that a breach has occurred.

3.2.2 Step 2 – Containment

Containment involves taking immediate corrective action to end the unauthorized practice that lead to a breach. For example, corrective action could include recovering the lost or stolen records; revoking/changing access codes or correcting weaknesses in an electronic security system. The main goal is to alleviate any consequences for both the individual(s) whose personal or confidential information was involved and JVS Toronto. All containment activities or attempts to contain the privacy breach shall be documented on the **Privacy Breach Report Form**.

3.2.3 Step 3 – Investigate

Once the privacy breach is confirmed and contained the Manager will conduct an investigation to determine the cause and extent of the breach by:

1. Identify and analyze the events that led to the privacy breach.
2. Evaluate if the beach was an isolated incident or if there is risk of further privacy breaches.
3. Determine who was affected by the breach e.g. clients or personnel, and how many individuals were affected.
4. Evaluate the effect of containment activities.
5. Evaluate who had access to the information.
6. Evaluate if the information was lost or stolen.
7. Evaluate if the personal or confidential information has been recovered.

3.2.4 Step 4 – Notify

The Manager shall consult with their Director who will consult with the Chief Privacy Officer to determine what notifications are required. Some considerations include:

1. Notification to authorities/other organizations. Examples include the police if theft or other crimes is suspected; credit card companies, financial institutions, the union, etc.
2. Does the loss or theft of information place any individual at risk of physical harm, stalking or harassment?
3. Is there a risk of identity theft? How reasonable is the risk?
4. Could the loss or theft of information lead to hurt, humiliation or damage to an individual's reputation?
5. Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

Timeline

Affected individuals should be promptly notified and receive the initial notification as soon as possible after the breach has occurred. Further communication with the affected individuals may occur during the process as updates occur.

Method

The method of notification will be guided by the nature and scope of the breach and in a manner that is reasonable to ensure that the affected individual will receive it. Direct notification e.g. by phone, letter, email or in person shall be used where the individuals are identified. Refer to **Sample Letter – Privacy Breach Response** if responding via letter. Where affected individuals are not fully known, media releases, website notices or letters to clients shall be considered. A report of findings and actions taken will be made by the Chief Privacy Officer.

Portions or all of the report may be shared with the affected party or parties whose information has been breached.

Responsibility for notification
If the breach was client information the manager of that program will provide the notification. In the event that the breach was personal information of JVS Toronto personnel, Human Resources will provide the notification.

In the instance where there is a high risk of adverse publicity as a result of the breach, the Chief Privacy Officer will be responsible for the notification. As necessary, a determination will be made if external media / public relations support is required due to the severity of the breach.

Notification will include:

- Description of the incident and timing
- Description of the information involved
- The nature of potential or actual risks or harm
- What actions were taken/are being taken
- Any appropriate actions for the individual(s) to take in order to protect themselves against harm
- A contact person for questions or to provide further information

3.2.5 Step 5 – Prevention of Future Breaches
Once the breach has been resolved, the Director will work with the Manager to develop a prevention plan or take corrective actions as required and will report back to the Chief Privacy Officer for required approvals. Prevention activities might include: audits; review of policies, procedures and practices; employee training; or a review of service delivery.

3.3 Supporting Documentation

Name	Location	Document Type
Privacy Breach Report Form	JVS Insider	PDF
Sample – Privacy Breach Response	JVS Insider	Word
Website Privacy Statement	JVS Insider www.jvstoronto.org/privacy-policy/	PDF

PRIVACY BREACH POLICY

SECTION 4 – GOVERNANCE

4.1 Policy Owner

Policy Owner	Director, Communications, Marketing & Quality (Chief Privacy Officer)

4.2 Version Control And Change History

Version Number	Approval Date	Approved by	Amendment
Version 6	n/a	n/a	This policy was edited on November 14, 2017 to change the position responsible for the Chief Privacy Officer.
Version 5	n/a	n/a	This policy was reviewed on December 22, 2016 and minor wording changes were made to reflect staffing changes and currently used internal terms.
Version 4	n/a	n/a	This policy was reviewed and edited on March 20, 2014 during the Imagine Canada accreditation process.
Version 3	n/a	n/a	This policy was reviewed and edited for formatting consistency on June 26, 2013.
Version 2	September 20, 2011	EMT pending	This policy has been developed as part of a full agency policy review.
Version 1	March 22, 2011		