BUSINESS & REMOTE OFFICE PRIVACY & SECURITY POLICY

Approved By	Executive Management Team
Last Reviewed	July 17, 2019 (next reviewed to be done within two years)
Responsible Role	Chief Privacy Officer (Manager, Business Analysis)
Responsible Department	Chief Privacy Officer

BUSINESS & REMOTE OFFICE PRIVACY & SECURITY POLICY

SECTION 1 - INTRODUCTION

1.1 Purpose
To ensure that all adhere to Privacy Principles who work at or act on behalf of JVS Toronto, including those who work at office locations and those who work remotely.

1.2 Scope
This 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
Business office	Any JVS Toronto location.
Chief Privacy Officer	A member of the JVS Toronto management team who is appointed with the responsibility for managing the privacy policies, inquiries, compliance, complaints, breaches, investigations, resolutions, practice modifications and implementation on behalf of the organization.
Confidential Information	Any information of a sensitive matter that should remain confidential.
Encrypt	To change information from one form to another especially to hide its meaning and to protect privacy.
Individuals who work for or act on behalf of JVS Toronto	Every individual working or volunteering at JVS Toronto including, but not limited to employees, managers, directors, senior management, casual and contract workers, volunteers, students, consultants, Board members, and Third Party Service Providers.
Personal Information	Under the Personal Information Protection and Electronic Documents Act (PIPEDA), personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • age, name, ID numbers, income, ethnic origin, or blood type; • opinions, evaluations, comments, social status, or disciplinary actions; and • Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).
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.
Remote office	Any location outside a JVS Toronto office where JVS Toronto is providing a service to a client, including an employee's premises or residential office.

1.4. Related Policies

1.4.1 Privacy Policies

1.4.2 Additional Policies
Code of Conduct Policy
Internet & Email Policy
Mobile Device Policy
Password Policy
Whistleblower Policy

1.5 Legislative Context
Child and Family Services Act
Health Care Consent Act
Personal Health Information Protection Act (PHIPA)
Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act
The Mental Health Act
The College of Psychologists of Ontario
The Ontario College of Social Workers and Social Service Workers

SECTION 2 - POLICY

2.1 Policy
Privacy and security protocols consistent with JVS Toronto's privacy policies apply to at all JVS Toronto locations and remote sites, including residential office locations. Privacy and security protocols regarding interactions with clients, information gathering, usage and security apply to the removal and transport of any files or documentation from any JVS Toronto location and all communication whether by telephone, e-mail, fax or other means.

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 All JVS Toronto Employees
Everyone who works at JVS Toronto, or acts on its behalf, is responsible to safeguard the privacy and security of files in their possession while working at a JVS Toronto office location, or remotely at work sites, such as schools, coffee shop, employer premises or a home office, by adhering to the following procedures.

3.2 Privacy at Workstations or Remote Office Locations
Ensure that there are no clients or visitors in open areas before speaking to a colleague about a client. Step into an office of meeting room and close the door to exchange client information between team members.

Ensure that only the files or documents immediately necessary for current work are on the surface of their workstation. When stepping away from your workstation, workspace or office during the day ensure the security of documentation to protect individual privacy and confidentiality. For example, when leaving your workstation for a meeting place confidential files and documents out of sight of passers by.

When working remotely without a dedicated space, secure files and documentation when leaving the work area. Place files or documents JVS Toronto entrusted to their possession in a workbag,

computer case or portable storage file container. Keep any files locked in an office, room or file cabinet overnight if returning to the location the next day.

Clear your work surfaces of files and documents at the end of each day, and lock all confidential files and documents in a desk drawer or file cabinet.

3.2.1 Working at a Home Office
When working at home, work in a secure environment with personal or confidential information not easily visible by others.

Do not dispose of documents while at home. Return any documents to JVS Toronto for proper and secure disposal according to JVS Toronto's **Records Retention & Destruction Policy.**

When working at home, work and store hard copy files securely in one area.

Do not use home phones to contact clients, employers or other JVS Toronto stakeholders, or provide them with a personal telephone number. In the case of special circumstances, individuals should use their judgment. For example, use a feature that blocks your caller identification.

Do not send JVS Toronto-related emails or documents from a personal or non-JVS Toronto e-mail address. Email personal or confidential information across a secure server using only JVS Toronto Webmail or VPN connection.

3.2.2 Meeting Clients in Public Spaces
When planning a meeting with a client in a public space, individuals must carefully consider the environment when choosing a place in which to meet with client, employer or other JVS Toronto stakeholder. Find a location that minimizes the likelihood that others will overhear conversation between the individuals.

Before beginning a client, employer or other JVS Toronto stakeholder meeting, ensure that the stakeholder is aware of the fact that their meeting is occurring in a public space and that although efforts made to minimize the likelihood that others will overhear conversation, there is no guarantee of privacy. Asked the stakeholder to decide if they would like to continue the meeting in the current location without the guarantee of privacy, or if they would like to reschedule the meeting at a JVS Toronto location. Document this conversation and stakeholder acceptance in case notes.

3.3 Removing Records from the Office
Only remove paper records containing personal or confidential information from the office when necessary in order to carry out job duties. Whenever practical, the original files will remain on-site and only copies removed. Identify duplicate documents as copies and destroyed when no longer needed. If originals are required, whenever possible, remove only relevant documents or an extract or summary.

Each department is responsible to create and maintain a sign-in/sign-out log with a due-back date to monitor removed files. The **Tracking Log for the Removal of Records Form** is for this purpose.

Return records to your JVS Toronto office as quickly as possible such as at the end of a meeting, the end of the day, or the end of a trip. Retain client files according to JVS Toronto's **Records Retention & Destruction Policy**.

Dispose of working documents containing personal or confidential information, such as draft client reports, in a confidential shredding box. Do not dispose of any JVS Toronto documents that contain personal or confidential information remotely

3.4 Transportation of Paper Records

Minimize the transportation of JVS Toronto documents to protect personal and confidential information. Whenever possible, scan and email the documents to your JVS Toronto email account to access them remotely through JVS Toronto webmail or take a photocopy of the document.

When transporting paper records containing personal or confidential information ensure:

- Documents are kept in an envelope or secured in a file folder
- Keep documents with you while in public or traveling by transit, cab, rail or plane.
- Lock documents in the trunk travelling by car or take the documents with you, such as stored under your seat, placed on your lap or beside you, or stored in carry-on luggage.
- Take precautions to block the view of onlookers when view personal and confidential documents while on public transit or in a public location.
- Temporarily store documents in a locked office or drawer if leaving a remote premise for meal breaks.

3.5 Off-Site Use and Transporting of Electronic Records

Refrain from viewing any personal or confidential document on your laptop while travelling on public transportation.

Store all electronic personal and confidential information on the JVS Toronto server when working remotely. When access to the JVS Toronto server is not available when working remotely, ensure you use one of these options to access and save documents.

1. **VPN software** to access and save documents on the JVS Toronto server.
2. An **encrypted** folder located on a JVS Toronto laptop.
3. An **encrypted** USB drive.

Your manager will request one of these options for you under the direction of the Director, Information Systems. Keep JVS Toronto computer and encryption devices with you at all times to prevent theft when working at non-JVS Toronto locations. When working at another JVS Toronto office, arrange for JVS Toronto computers and encryption devices to be stored in a locked office or file cabinet when not in use.

Place all documents saved in an encrypted folder of USB drive on the JVS Toronto server when you return to the office. When working remotely for longer periods, save documents to the JVS Toronto server on your next visit to a JVS Toronto office.

When working remotely using a JVS Toronto laptop, or another computer, logged off and/or shut down the computer when not in use. Do not leave personal or confidential information on the screen when away from the computer. All laptops are password protected and set-up so that after a set amount of inactivity, the laptop will lock and requires a password. JVS Toronto laptops are for employee use only.

Never save any JVS Toronto work on the desktop of personal laptops or computers. Ave all electronic files on the JVS Toronto network, an encrypted USB drive or encrypted file folder.

Faxing, Photocopying and Printing
When faxing documents with personal or confidential information, verify that the fax number is correct, place a cover sheet over the document, and ensure someone is available to receive the fax before sending.

Ensure security of photocopied material by remaining until completed, and remove originals from the photocopier, particularly when printing documents with personal or confidential information.

3.5.1 Laptops
Transport laptops in a proper laptop bag to protect the laptop, its software, and contents.

Laptop Bags
Place your business card in the identification holder or in a pocket of the laptop bag for identification purposes. Laptops for program use have identification as property of JVS Toronto.

Passwords
Do not include in a laptop case a document containing the user's IDs, passwords, account numbers, and other security information.

Strategize for Separation
Think about strategies for times when brief separation from a laptop case may occur.
Hold it. Place it on your lap, under the seat or beside you when by transit, cab, train or plane.
Hide it. Never leave a laptop in plain sight in a car. Lock it in the trunk or hide it beneath a seat.
Vault it. In a hotel, see if a safe is large enough to hold a laptop is available, or hide it in a drawer or closet.
Airport security practices. Send items through x-ray machine in reverse order of the value: shoes, books and papers, the laptop-less case, jacket, and lastly, the laptop.

3.5.2 Email and Mobile Device Communication of Private information

Email
Do not use personal or non-JVS Toronto email to transmit personal or confidential information related to stakeholders. Use JVS Toronto secure methods to email personal or confidential information across a secure server using only JVS Toronto Webmail or VPN connection.

Emailing personal or confidential information is not secure unless both parties are using JVS Toronto email accounts. When emailing electronic documents with personal or confidential information to a non-JVS Toronto email address, password protect the document. Share the password with the recipient by phone or in a separate email.

Password Protecting Microsoft Office Documents
Open the **Microsoft Office file** you want to **protect**.

- Click **File**.
- Click **Info**.
- Click **Protect Document**.
- Click Encrypt with **Password**.
- Enter a **password** and click OK.
- Confirm your **password** and click OK.

Mobile Devices
Use mobile phones and other devices in accordance with JVS Toronto's **Mobile Device Policy.** Do not text or instant message any personal or confidential information.

3.7 Loss or Theft Reporting

Report a loss or theft of JVS Toronto documentation or devices that may contain personal or confidential information, immediately to your manager who will contact the Chief Privacy Officer.

When a mobile device used for JVS Toronto-related work and paid for in part or total by JVS Toronto, is lost or stolen, call JVS Toronto's Desktop Support (currently XBASE (416) 340-1020) immediately; then inform your manager to assist with the issue.

Failure to comply with the practices, processes and conduct outlined above may result in disciplinary action up to and including termination of employment and/or the individual's relationship with JVS Toronto.

3.8 Supporting Documentation

Name	Location	Document Type
Tracking Log for the Removal of Paper Records	JVS Insider	PDF

SECTION 4 – GOVERNANCE

4.1 Policy Owner

Policy Owner	Chief Privacy Officer

4.2 Version Control and Change History

Version Number	Approval Date	Approved by	Amendment
Version 9	n/a	n/a	This policy was reviewed and edited for clarity on July 17, 2019.
Version 8	n/a	n/a	This policy was reviewed and edited for wording additions on August 10, 2018.
Version 7	n/a	n/a	This policy was edited on November 14, 2017 to change the position responsible for the Chief Privacy Officer
Version 6	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 5	n/a	n/a	This policy was reviewed and edited on March 20, 2014 during the Imagine Canada accreditation process.
Version 4	n/a	n/a	This policy was reviewed and edited for formatting consistency.
Version 3	September 20, 2011	EMT	This policy has been developed as part of a full agency policy review.
Version 2	April 2011	Reviewed	
Version 1	December 2007		