BUSINESS & REMOTE OFFICE PRIVACY & SECURITY POLICY

Approved By	Executive Management Team
Last Reviewed	August 10, 2018 (next reviewed to be done within two years)
Responsible Role	Chief Privacy Officer (Director, Communications & Marketing)
Responsible Department	Chief Privacy Officer

BUSINESS & REMOTE OFFICE PRIVACY & SECURITY POLICY

SECTION 1 - INTRODUCTION

1.1 Purpose
To ensure that Privacy Principles are adhered to by all 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 executive management team who is appointed with the responsibility for managing the risks and business impacts of privacy laws and policies.
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. This is done 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	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.
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
Client Records Collection & Disclosure Policy
JVS Toronto Personnel Records Collection & Disclosure Policy
JVS Toronto Enterprise Privacy Policy
Privacy Breaches Policy
Privacy Complaint Resolution Policy
Records Retention & Destruction Policy

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
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

SECTION 2 - POLICY

2.1 Policy
Privacy and security protocols consistent with JVS Toronto Enterprise Privacy Policy will be fully adhered 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 will 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 (e.g. schools or coffee shop) or a home office, by adhering to the following procedures.

3.1.1 Privacy at Workstations or Remote Office Locations
Individuals must ensure that only the files or documents immediately necessary for current work are on the surface of their workstation. An individual who leaves their workstation, work space or office during the day will use "common sense" to help to ensure the security of individual privacy and confidentiality. For example, an individual who is leaving their workstation for a meeting will place confidential files and documents out of sight of passers by.

Individuals who are working remotely, but who do not have a dedicated space, will secure files and documentation when leaving their assigned work area. This may require an individual placing files or documents entrusted to their possession in a locked brief case, or in a locked portable storage file container.

Individuals will clear their work surfaces of files and documents at the end of day, and ensure that all confidential files and documents are securely placed in a locked drawer or file cabinet.

3.1.1 (a) 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. Ensure any documents are returned to JVS Toronto for proper and secure disposal according to JVS Toronto's **Records Retention & Destruction Policy.**

- When working at home, employees will 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 caller identification).

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

3.1.1 (b) 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 conversation between the individuals will be overheard by others.

- Before beginning a client, employer or other JVS Toronto stakeholder meeting, individuals will ensure that the stakeholder is aware of the fact that their meeting is occurring in a public space and that although efforts have been made to minimize the likelihood that conversation will be overheard by others, privacy cannot be guaranteed. The stakeholder will then be asked 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. The nature of this conversation will be documented in the stakeholder file.

3.2 Removing Records from the Office

Individuals working for or acting on behalf of JVS Toronto will only remove records containing personal or confidential information from the office when absolutely necessary to carry out their job duties. Whenever practical, the original files will remain on-site and only copies removed. Copies will be clearly identified as such 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** can be used for this purpose.

Return records to a secure environment as quickly as possible, for example, at the end of a meeting, the end of the day, or the end of a trip.

Regarding client files, ensure that all working copies of paper files containing personal or confidential information are returned to the office or a secure environment no later than within *10 business days of closing the client's file*. Returned files are to be securely retained according to JVS Toronto's **Records Retention & Destruction Policy**.

Documents containing personal or confidential information that do not need to be retained (ie. draft client reports), must be disposed of in a secure manner so that the record may not be reassembled and read. Records containing personal or confidential information will never be discarded remotely, but returned to JVS Toronto for proper and secure disposal according to JVS Toronto's **Records Retention & Destruction Policy**.

3.3 Transportation of Paper Records
In order to protect the personal and confidential information contained in paper records, transportation of paper records will be minimized. Whenever possible, the required paper documents will be scanned and a copy e-mailed through the JVS Toronto server to a JVS Toronto account. This information can then be accessed through JVS Toronto webmail.

3.3.1 Transporting of Electronic Records
As noted previously, whenever possible, only copies of paper files will be transported.

When paper records containing personal or confidential information must be transported, the following will be followed.

- Paper records will be securely packaged and kept under the direct control of the individual while in public such as in a coffee shop or using public transit.

- When an individual travels by car, paper records will always be locked in the trunk. Unless there is no alternative, paper records should not be left unattended in a car trunk while the individual goes elsewhere.

- Paper records will not be opened or reviewed in pubic (e.g. while on public transportation or in a restaurant).

- Individuals, who travel by cab, subway, bus, train, or airplane, will always ensure that files are in their physical presence. This means that in a cab or on a subway, bus or train, files will be in a locked brief case on the individual's lap so that they are not left on the seat, or in the trunk of the cab; on a plane, documents should taken on board and stored with the individual as carry-on luggage.

- When working at other locations outside the office, paper records will be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, the records will be temporarily stored in a secure location, such as a locked room, desk drawer, or filing cabinet.

3.4 Off-Site Use and Transporting of Electronic Records

- Due to the potential for privacy breaches, unencrypted devices or computer hard drives (personal or work and laptops or desktops) may not be used to store JVS Toronto work. Electronic personal and confidential information must be stored on the JVS Toronto server.

- When transporting electronic files, or working remotely with a work laptop that is not connected to the JVS Toronto server, one of the following options must be used:

1) Members of the senior management team and others as approved who utilize work laptops may use **VPN software** to securely access the JVS Toronto server from any remote location with internet access.

2) JVS Toronto employees who regularly use a JVS Toronto work laptop off-site (with or without internet access) will save all their work on an **encrypted** folder on their JVS Toronto laptop.

3) JVS Toronto employees who work on a non-regular basis off-site will use an **encrypted** USB drive for transporting and saving their work. This method is also suitable for individuals using personal laptops or desktop computers.

- The manager or JVS Toronto contact will decide in consultation with Information Systems, on which secure method of storage will be used.

- To prevent loss or theft, the USB drive/laptop will be kept under the constant control of the individual while in transit.

- When working at any remote location, the USB drive/laptop will be kept under the constant control of the JVS Toronto individual and stored and locked in a filing cabinet or desk drawer after use.

- Individuals using either an encrypted folder or USB drive must ensure their data is placed on the JVS Toronto server once a month to protect against the loss of that data.

3.5 Internal and External Communication of Private information

3.5 (a) Email

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

When e-mailing electronic documents with personal or confidential information to a non-JVS Toronto email address, the document must be password protected following the JVS Toronto **Password Policy.**

3.5 (b) Laptops

Laptops will be transported in a proper laptop bag to protect the laptop, its software, and contents.

3.5 (c) Computer Bags

A JVS Toronto business card or other ID tag should be affixed to a strap of the bag. Use internal pockets to store more ID. Put only the individual's name, and JVS Toronto phone number and e-mail address on the tags. Add the phrase "Reward for Return" to the ID tags.

3.1.5 (d) Passwords

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

3.5 (e) Strategize for Separation

Think about strategies for times when brief separation from a laptop case may occur. Hold onto the laptop when in a taxi or when traveling on an airline.

- **Hide it.** Never leave a laptop in plain sight in a car. Move it to the trunk — if sure no one is watching — or hide it beneath a seat.
- **Vault it.** In a hotel, see if a safe large enough to hold a laptop is available.
- **Airport security and x-rays:** Send items through the x-ray machine in reverse order of the value: shoes, books and papers, the laptop-less case, jacket, and lastly, the laptop.

If it is necessary to view personal or confidential information on a laptop screen when working at locations outside the office, ensure that the screen cannot be seen by anyone else. Personal or confidential information should never be viewed on a laptop screen while travelling on public transportation.

- When working at home or at another remote location, a laptop or home computer will be logged off and/or shut down when not in use. Do not leave personal or confidential information on the screen when away from the computer. All laptops will be password protected and set-up so that after a set amount of inactivity, the laptop locks and requires the password to be entered.

- Do not share a laptop that is used for work purposes with other individuals, such as family members or friends.

- Never save any JVS Toronto work on the desktop of personal laptops or computers. Electronic files are to be saved on the JVS Toronto network, or an encrypted flash drive. If any exception is desired, manager approval is required.

3.6 Mobile Devices

- Mobile phones and other devices must be used in accordance with JVS Toronto's **Mobile Device Policy.**

- Personal or confidential information cannot be sent via email, unless both parties are using JVS Toronto email accounts.

- Personal or confidential information cannot be sent using texting or any form of instant messaging.

3.7 Faxing, Photocopying and Printing

- Avoid faxing personal or confidential information if possible. It is recommended that instead documents with personal or confidential information be scanned and emailed over the JVS Toronto secure network. If documents with personal or confidential information must be faxed, check and recheck the number, use a cover sheet and ensure someone is available to receive the fax before sending.

- Ensure security of photocopied material by remaining at the copier until the copying is completed, and ensuring that all originals are removed from the photocopier.

- When printing confidential material or documents with personal or confidential information, ensuring that the material is picked up immediately upon printing. As well, do not look at documents that have been printed by others.

3.8 Loss or Theft Reporting

A loss or theft of documents with personal or confidential information either in hard copy files, laptop/soft copy (such as an encrypted flash drive), or mobile devices will be reported immediately to a member of JVS Toronto management who will initiate a **Privacy Breach Report**.

When a cell phone that is 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 and report the device as lost or stolen. If the loss occurs outside of office hours, leave a message with contact details. If not contacted during the next business day, contact JVS Toronto's Facilities Manager, who will assist in escalating 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.

3.2 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 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		