

Employee Privacy and Confidentiality Policy

1. Overarching Principles

Vector is committed to protecting the privacy of individuals that it comes in contact with and/or employs. Vector employees who disclose personal information contrary to this Employee Privacy and Confidentiality Policy (“**Policy**”) may be subject to disciplinary measures, up to and including termination for cause. Vector employees (as hereinafter defined) are required to:

- ensure that personal information to which they may have access remains confidential, is only used for the purposes for which it was collected, and is not disclosed without authorization or used for personal purposes;
- follow all procedures regarding collection, use, and disclosure of personal information as set out in this Policy as well as any other policy or procedure that may apply to the management of Vector employees’ and/or customers’ personal information.

Vector’s Chief Operations and Financial Officer is accountable for the implementation of this Policy. Any issues or questions regarding this Policy should be directed to the Chief Operations and Financial Officer.

2. Purpose

The purpose of this Policy is to preserve the privacy of Vector’s employees, as well as other individuals about whom Vector may collect personal information (such as representatives of Vector’s emergency contacts, graduate students, postdoctoral fellows, visiting researchers, and those registering for events and courses), by outlining employee obligations and procedures for dealing with the collection, use, disclosure, and retention of personal, privileged, or confidential information.

3. Scope

This Policy applies to all Vector employees accessing personal information when performing their duties.

4. Definitions

In this Policy:

“**collect**” means to gather, receive, or record personal information from any source and by any method;

“**disclose**” means to make personal information available to a person other than a Vector employee or its authorized representatives;

“**Vector employee**” means an individual who is or was employed by Vector (this includes any current, past or prospective employee), as well as faculty members, research scientists, consultants, or contracted staff of Vector.

“**personal information**” as used in this Policy, is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, personal telephone number, any numerical identification (such as a Social Insurance Number),

and credit information. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include “business contact information”, which is defined as “any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment”, including the usual data elements such as name or title, work address, work telephone number, work fax number, or work email address.

“third parties” (or “third party”) are individuals or organizations other than the subject of the records or representatives of Vector.

“use” means the management of personal information by or on behalf of Vector.

5. Why Vector Collects and Manages Personal Information

Vector collects, uses, and discloses personal information of Vector employees:

- to verify employees’ identity;
- to make decisions regarding employment applications, including to conduct relevant pre-employment references or other background checks;
- to meet payroll processing requirements;
- to evaluate job performance and skills and make decisions about assignments, training, and compensation;
- to supervise, provide, determine, and record eligibility for, and to manage, employee benefit plans or programs;
- to manage disciplinary matters and to establish, manage, and terminate an employment or contractual relationship;
- to maintain a safe workplace and to manage health and safety issues, including where a medical condition, illness, or injury affects an employee’s work or ability to work, and/or workers’ compensation claims;
- for any post-employment related activities of Vector in respect of a Vector employee, including the provision of references;
- to provide adequate information to third parties to whom Vector has outsourced any of these tasks;
- to respond to inquiries about employee programs, services, or other matters;
- to record significant events during the employment relationship;
- to organize staff recreational activities;
- to send employees electronic messages in connection with their employment;
- to meet legal, security, or regulatory requirements or for fraud management purposes;
- to conduct internal reviews, audits, investigations, and complaint resolution processes; and/or
- to facilitate and monitor the use by employees of Vector’s facilities, equipment, devices including email, Internet, and intranet access.

6. How Vector Obtains Employees' Consent

Generally, when prospective Vector employees accept an offer of employment from Vector, their consent to the collection, use, and disclosure of their personal information is understood to be given for all purposes that have been identified to them verbally or in writing, including the purposes detailed in this Policy.

When applicants respond to an advertisement or notice of job opportunity, or otherwise submit a resume for employment, they consent to the collection, use, and disclosure of the personal information they provide (or personal information provided by third parties, such as references they have provided or in the context of background checks, but only when authorized by law) for the purposes of evaluating their suitability for the job .

In addition, and from time to time, a Vector employee may be requested to consent to the collection, use and disclosure of personal information for further purposes not included in any consent previously given e.g., for registration in an employee benefits program or group registered retirement savings plan.

7. Exceptions

Vector may use personal information without knowledge or consent of its employees if it is used for the purposes authorized under applicable law and/or for the purpose of acting in respect of an emergency that threatens the life, health, or security of an individual, or if obtaining consent would defeat the purpose for which information is being collected, such as in connection with investigations of an offence under applicable law.

Vector may also collect, use, and disclose personal information without the knowledge or consent of the employee if it is clearly in the interests of the individual and consent cannot be obtained in a timely way.

8. Sources of Employee Information

Personal information may be collected from any of the following sources, to the extent authorized by law: resumes, job applications, interviews, personal information forms, payroll-related documents, reference checks, and other background checks, performance appraisals, medical certificates from attending physicians, benefit application forms, emails and computer use and records, telephone, faxes, leave of absence requests, vacation or maternity and parental leave requests, investigations into complaints, publicly available sources or entities with which Vector has a partnership, such as an institution e.g., a hospital or university.

9. What Employee Personal Information is Collected

Personal information collected about Vector employees includes the following information:

- Information received from Vector employees on applications or other forms, for instance, applications for employment or for employment benefits, such as gender, age, birth date, home address, and personal telephone numbers, e-mail addresses, next-of-kin or other emergency contact information, Social Insurance Number, driver license number, bank and account information, marital status, names, addresses and ages of dependants, language preference, education and training, employment history, references, and records of offences as well as emergency contacts, severe allergies, or medical conditions that require our awareness;
- Information related to the Vector employee's employment, such as position, promotions, employee identification number, work history, full-time/part-time status, scheduled hours, hire date, performance details and/or appraisals, disciplinary records, salary, bonus, benefits, perquisites, termination date, and associated details (e.g., voluntary or involuntary and documentation);
- Information received from Vector employees on a voluntary basis when Vector conducts surveys of their preferences, needs, or interests, at all times in accordance with the methodology included in such surveys;

- Information submitted by Vector employees in connection with any claim for benefits under any of Vector's employee benefit plans or programs (including employee relocation assistance and wellness benefit), or workers' compensation and information required for administration of payroll, benefit plans, group insurance plans, and group retirement savings plans; and
- Information required for security purposes and/or any information authorized and/or required by law.

10. How Employee Personal Information is Maintained

Vector maintains a personal file for each Vector employee. The information contained in these files is gathered and collected for employment purposes. Contents of these files generally include information regarding employment letters, promotions, transfers, performance and salary reviews, medical notes (if applicable), and other documentation. These files are kept strictly confidential in accordance with the security safeguards detailed in section 13 of this Policy.

11. Access to Vector's Employee Personal Information

Access by employees to their personal file is permitted at reasonable intervals within 30 days (where possible) of employees' written request to the Manager, Human Resources. The Manager, Human Resources will be present when the employee views his/her file. In certain circumstances, it may be necessary for Vector to limit the employees' access to part of his/her employee file where such documents would disclose information that is the subject of legal proceedings or arbitration, information protected by privilege, third party personal information, or if granting access would threaten the employees' safety or health. Vector employees may obtain a copy of any document in their file that they have signed previously. No material contained in a file may be removed from the file. For greater certainty, Vector shall not have to create or reconstitute information not already in its possession when complying with employees' access requests.

If there is inaccurate personal information in the employee's file, the employee must advise the Manager, Human Resources of the correction, and Vector will amend the record accordingly. If Vector concludes that a correction is not warranted (for example, if Vector believes the information to be accurate or if the information is of a subjective nature), the employee will be permitted to attach a notation to the file.

12. Sharing of Vector Employees' Personal Information

To the extent allowed by law, by this Policy, by the Chief Operations and Financial Officer and/or by the employee's consent and as required for a stated purpose, Vector may disclose personal information to any of the following third parties: outside payroll administrators, outside reference check agencies, private investigators, potential employers conducting reference checks, benefits administrators, solicitors, purchasers or potential purchasers of the business, trustees in bankruptcy, insurance companies, consultants in the employment areas, and law enforcement agencies.

More specifically, Vector may share its employees' personal information under certain circumstances, such as:

- when the employee has consented to the disclosure;
- to Vector's partners and to Vector employees with a need to know, when there is a business reason to do so;
- to government agencies with a need to know (e.g., to respond to Employment Insurance inquiries, disclosure under the *Public Sector Salary Disclosure Act, 1996*, etc.);
- when the employees' health information or diagnosis is necessary to allow Vector and/or the health benefits provider to manage the employees' absences or health benefits, as the case may be;
- if we engage a third party to provide administrative services (e.g., audit services, maintenance services to our computer network, payroll services, benefits provision) and the third party's privacy and security standards meet our requirements;

- when required to perform reference or other relevant background checks;
- when contacted by a third party requiring information in the context of background verifications, Vector may disclose limited factual information such as the employee's job title, employment status, working hours per week, number of years of service, date of hiring and termination, or any other factual information that would otherwise be available through another source without any breach of applicable law, unless Vector has obtained the employee's consent to release more information;
- when Vector is required or authorized to do so by law, for example, in the event of an emergency that threatens the employee's life, health, or security, or in order to investigate a breach of an agreement or a contravention (or anticipated contravention) of a federal or provincial law or for the purpose of detecting or suppressing fraud, in accordance with applicable law; and
- as part of an application for a grant, subsidy, or program.

Notwithstanding the foregoing, Vector will cooperate with law enforcement agencies and will comply with any court order or law requiring disclosure of personal information without its employee's consent.

13. Safeguards with Respect to Vector Employee Personal Information

Vector maintains adequate security systems to secure personal information that is collected, used, retained, and disclosed taking into consideration the level of sensitivity including physical measures such as locking cabinets, electronic security, and organizational systems. All Vector employee personal information will be treated as confidential and only used by Vector or disclosed to third parties in accordance with the terms on which it was collected and its intended purposes, except as permitted or required by law or this Policy.

Vector uses contractual arrangements to provide a comparable level of protection where information is processed by a third party for payroll and benefits administration or for other purposes e.g., attendance tracking. Vector uses reasonable measures to ensure that third parties will only use your information for the purposes specified.

14. Transfer of Vector Employee Personal Information Outside of Canada

In some cases, Vector employees' personal information may be disclosed, processed, and stored outside Canada, and therefore may be available to government authorities under lawful orders and laws applicable there. Any questions you have concerning the handling of your personal information by the non-Canadian service providers can be addressed to our Chief Operations and Financial Officer whose contact information can be found at the end of this Policy.

15. Retention of Personal Information

Vector will retain certain personal information in order to satisfy the purpose for which it was collected, to satisfy our legal obligations and to protect the interests of Vector. Despite the foregoing paragraph, personal information that is the subject of a request by an individual or a government authority, or the object of a litigation, shall be retained as long as necessary to allow individuals or Vector, to exhaust any recourse they may have under applicable laws.

16. Vector Employees' Responsibility with Respect to Personal Information

Exercising care when handling confidential information concerning Vector's activities must be the concern of all Vector's employees.

Personal, privileged, or confidential information about employees and other individuals that interact with Vector may only be collected, used, disclosed, and retained for the purposes identified by Vector as necessary.

Vector employees are forbidden to consult information if not necessary to their work.

Caution must be exercised in discussing personal information outside the office, especially in the presence of anyone not connected with Vector or not authorized to have access to the information. Special care should be exercised in elevators and other public places to ensure that casual conversations or inadvertent displays of written material do not lead to the release of such information. Care should also be taken in conversations within Vector to avoid leaks of non-public information to those who do not have a bona fide “need to know”. Vector depends on all employees to exercise the care necessary to ensure that the confidentiality of customer information is maintained at all times.

Vector employees are responsible for:

- keeping their own employee files current regarding name, address, phone number, and dependents;
- being familiar with Vector’s policies and procedures regarding personal information; making sure to obtain the proper consents and authorizations prior to disclosure of personal, privileged or confidential information;
- immediately reporting any breaches of confidentiality to Manager, Human Resources or Chief Operations and Financial Officer.
- keeping private passwords and access to personal, privileged, or confidential data;
- returning to Vector all work-related, privileged, confidential or customer information in their possession before or immediately upon termination of employment.

Senior Management is responsible for:

- ensuring policies and procedures regarding collection, use, and disclosure of confidential information or personal information are consistently adhered to;
- responding to requests for disclosure after the proper release is obtained;
- attending any privacy compliance training, as requested from time to time;
- obtaining from terminating Vector employees prior to their termination any work-related, privileged, confidential, or customer information in their possession; and
- ensuring that disclosure of employee personal information to a third party is done with the approval of the Manager, Human Resources or Chief Operations and Financial Officer in order to minimize risk of non-compliance with applicable legislative or regulatory regimes as well as with this Policy.

The Manager, Human Resources, is responsible for:

- ensuring that appropriate consents have been obtained from Vector employees with respect to the collection, use, and disclosure of personal information;
- observing all security measures;
- ensuring systems are maintained and procedures in place to ensure employee records are kept private;
- obtaining the proper consents and authorizations prior to disclosure of information contained in employee records;
- responding to Vector employees’ requests for access to their files;
- ensuring proper disposal of unnecessary files or information in accordance with any data retention policy;

- attending any privacy compliance training, as requested from time to time;
- internal compliance with applicable policies or legislation;
- monitoring and responding to third party requests for personal information; and,
- where collection, use or disclosure is permitted without prior consent, notifying individuals of the collection, use, and disclosure of personal information after such occurrence.

17. Complaints Procedures

Concerns or complaints related to data protection or privacy issues must be made, in writing, to the Chief Operations and Financial Officer setting out the details of the concern or complaint.

The Chief Operations and Financial Officer shall investigate the matter forthwith and make a determination related to the resolution of the concern or complaint.

If your concerns remain unresolved, you can contact Vector's President & CEO at the coordinates below:

Garth Gibson, President & CEO
Vector Institute
MaRS Centre, West Tower
661 University Ave, Suite 710
Toronto, ON
M5G 1M1
Email: ceo@vectorinstitute.ai

18. Changes to this Employee Privacy and Confidentiality Policy

Vector regularly reviews all of its policies and procedures, and we may change this Policy from time to time.