Centre for Education & Training™
The Power of Change. The Passion for Growth.

PRIVACY AND CONFIDENTIALITY POLICY

PURPOSE

The Quality Continuous Improvement Centre for Community Education and Training, operating as the Centre for Education & Training (TCET) is committed to protecting the privacy of its clients, students, volunteers, employees, funders and other stakeholders. We value the trust of those we deal with and recognize that maintaining this trust requires that we be transparent and accountable in how we treat the information they choose to share with us.

During the course of managing our various programs, services, projects and conducting our business activities, we frequently gather and use personal, privileged and/or confidential information which may relate to employees, company operations or clients/customers. Anyone from whom we collect such information should expect that it will be carefully protected. The purpose of this Policy is to ensure that TCET employees know their obligations and are aware of the procedures for dealing with personal, privileged and/or confidential information.

Employees are required to follow all procedures regarding the collection, use and disclosure of personal information as set out in this Policy. Employees who disclose personal information in contravention of this Policy will be subject to disciplinary measures, up to and including dismissal for cause.

When in doubt as to whether certain information is confidential or personal, no disclosure should be made without first asking the Chief Operations Officer / Chief Privacy Officer. This basic policy of caution and discretion in handling of personal and confidential information extends to both external and internal disclosure.

The Chief Operations Officer also acts as Chief Privacy Officer (COO/CPO) and is accountable for the implementation of this Policy. Any issues or questions regarding this Policy should be directed to the COO/CPO who may be contacted at rolson@tcet.com

SCOPE

This Policy applies to all employees, contractors, subcontractors of TCET or anyone else who is granted access to personal, privileged and/or confidential information.
This policy works in conjunction with:

- Access to Personnel Files Policy
- Data Security Policy
- Technology Use Policy
- Internet and Email Use Policy
- Social Media Policy
- Records Retention and disposal Policy

DEFINITIONS

- **General employee information**: means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationships between the organization and that individual, but does not include personal information that is not about an individual's employment.
- **Personal information:** broadly speaking, it includes any information that can used to identify an individual or as defined in applicable Canadian privacy laws. It may include race, ethnic origin,

colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. 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 and certain publicly available information such as name, job title, job description.

- **Personal health information** is information about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision-makers on behalf of the individual.
- **Third party** is an individual or organizations other than the subject of the records or a representative of **TCET**. Note that in certain circumstances, **TCET** may be entitled to provide personal information to a third party acting as an agent of **TCET**.
- **Service provider** means any organization, including, without limitation, a parent corporation, subsidiary, affiliate, contractor or sub-contractor, that directly or indirectly, provides a service for or on behalf of **TCET**.

POLICY

You have an obligation to safeguard the personal and business information entrusted to us by our clients, employees, suppliers, service providers and others, as well as the confidentiality of TCET's own affairs. This obligation continues even after you leave TCET.

- Obligation to protect personal and confidential information
    - Clients, employees, suppliers, service providers and others trust TCET to keep their personal information and confidential business information safe and secure. Protecting their privacy and the confidentiality of their dealings with us is essential to safeguarding our business operations, financial well-being and reputation. Protecting personal and confidential information is also a legal requirement under Canadian privacy laws.
    - You are expected to be aware of, and follow the policies and procedures that TCET has put in place to protect personal and confidential information, to comply with applicable laws and regulations and so that you know how to report, respond to and remediate any breach of privacy or confidentiality.
    - All information about or received from clients, employees (including prospective clients and employees) or other individuals should be presumed to be confidential information unless otherwise explicitly stated. Keep in mind that even a seemingly harmless or helpful disclosure of client or employee personal information (such as to a client's family member) could be a breach of this Policy and can have serious consequences for you, TCET and the individuals involved.
    - Never access client or employee personal information, or confidential business information about TCET or a client, without a legitimate business reason and proper authorization. Employee "snooping" into files of clients or other employees is strictly prohibited. For example, you may not view client profiles or account information of family members, friends or acquaintances without a valid business reason to do so. TCET monitors employees'

access to and use of information technology services and physical storage facilities in order to prevent and detect improper access to information. Employee snooping is a breach of Canadian privacy laws and this Policy, and could result in disciplinary action, up to and including termination of employment and legal proceedings against you by TCET and the affected individuals.

- Appropriate handling of personal and confidential information includes the following:

    - Follow appropriate procedures and processes for storing and controlling access to electronic and physical confidential information. All private and/or confidential physical information should be stored in locked cabinets or drawers. Please refer to the Technology Use and Data Security Policies.
    - Follow appropriate procedures for transmitting confidential information. Do not send confidential information via non-secure media, platforms or internet connections (e.g., WiFi, Dropbox, Google Drive, etc.). Please refer to the Technology Use and Data Security Policies on secure transmission via fax, email and/or the Internet.
    - Do not carelessly display confidential information (for example, by leaving it visible on a computer monitor, or leaving confidential documents where they could be viewed, lost or stolen).
    - Keep private all passwords and access to personal, privileged and/or confidential data.
    - Do not disclose confidential information to persons outside TCET (including family or household members or close associates) or to other employees who do not require the information for their work.
    - Take care when discussing confidential information where it might be overheard or intercepted (such as when using a cell phone) - for example, by confirming to whom you are speaking and ensuring that your conversation cannot be overheard by unauthorized persons. Never discuss confidential information in social settings, such as restaurants, elevators, trains and other public places.
    - Destroy or dispose of information/documents in a secure manner, such as using the secure shredding equipment available at all TCET locations according to security requirements and policies and procedures for document retention and destruction.
    - Relinquish any personal, privileged, confidential or client information in your possession before or immediately upon termination of employment.

Employees or Contractors who work from an off-site location, or those who take work home, even on an occasional basis, must be particularly vigilant in safeguarding confidential, sensitive or personal information pertaining to the Company, its clients and/or employees.

It is your responsibility to safeguard and appropriately handle any personal or confidential information which you have custody of or access to, or which you use. This is the case even when you are disposing of waste or damaged materials. If you become aware of a breach of privacy or confidentiality, immediately report it to your Supervisor/Manager, the COO / CPO or, where appropriate, under the Whistleblower Policy, so that steps can be taken to prevent, minimize or mitigate any negative impact on clients, employees or TCET.

- Disclosures of personal and confidential information to third parties

  Third parties sometimes request information about clients (including family and friends). Subject to legal exceptions, you must obtain the consent of the client before releasing a client's personal or confidential information held by TCET. This includes releasing information about whether or not an individual, business or government department is actually a client. In some cases, you may need assistance from your Supervisor/Manager, a member of the Senior Leadership Team or the COO / CPO to verify if a demand for information has been properly made and documented to permit or compel you or TCET to provide information under the law without client consent. You should also be alert to situations where legal requirements may prohibit you from telling the client about a demand for information.

Employee Information

a) Appropriate consents and authorizations will be obtained from employees with respect to the collection, use and disclosure of general employee information, personal information and personal health information;
b) Where collection, use or disclosure is permitted without prior consent, individuals will be notified after such occurrence;
c) Proper storage practices, such as locked cabinets, drawers and/or offices will be utilized to ensure all employee records are kept private;
d) Personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within **seven (7) years** after its use;
e) Proper disposal practices will be utilized to discard or destroy any unnecessary files / information / documents in a secure manner, such as using the secure shredding equipment available at TCET locations;
f) Employees may request and be granted access to their general employee information records (employee file) and may request correction(s) to be made, if applicable;
g) Separate files will be maintained to ensure that personal and personal health information are protected;
h) Authorization from the COO / CPO will be obtained prior to disclosure of personal information and personal health information to a third party in order to minimize risk of non-compliance with applicable legislative or regulatory regimes.

Client Information

a) Personal, privileged and/or confidential information about customers and clients may only be collected, used, disclosed and retained for the purposes identified by TCET as necessary and only after such purpose has been disclosed to customers and clients prior to collection, and their consent obtained.
b) Employees must ensure that no personal, privileged and/or confidential client information is disclosed without the client's consent and then only if security procedures are satisfied.
c) Client information is only to be accessed by employees with appropriate authorization and for legitimate business reasons.
d) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within **twelve (12) months** after its use.

Notwithstanding the above, personal information that is the subject of a request by an individual, a regulatory agency or law enforcement shall be retained as long as necessary to allow individuals to exhaust any recourse they may have under applicable Canadian privacy laws.

Concerns or complaints related to privacy issues must be made, in writing, to the COO / CPO who shall investigate the matter forthwith and make a determination related to the resolution of the concern(s) or complaint(s).

No employee shall be disadvantaged or denied any benefit of employment by reason that TCET believes that an employee will do anything referred to in paragraphs (a), (b), or (c) below or by reason that an employee, acting in good faith and on the basis of reasonable belief:

(a) has disclosed to the Privacy Commissioner of Canada (or other applicable Canadian privacy regulatory body) that **TCET** or any other person has contravened or intends to contravene a provision of *Personal Information Protection and Electronic Documents Act* ("PIPEDA") (or other applicable Canadian privacy laws) related to the protection of personal information;
(b) has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA (or other applicable Canadian privacy laws)related to the protection of personal information;
(c) has done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA (or other applicable Canadian privacy laws) related to the protection of personal information not be contravened.

The Privacy Commissioner of Canada (or other applicable privacy regulatory body) shall be notified without delay of any incident involving the loss of or unauthorized access or disclosure of personal information under **TCET's** control where there is a reasonable risk of significant harm to an individual as a result of the loss, access or disclosure.

In the event that TCET uses a service provider outside Canada to collect personal information about an individual for or on behalf of TCET or TCET, directly or indirectly, transfers to a service provider outside Canada personal information that was collected with the individual's consent, the individual will be notified in writing or orally of:

- the way in which the individual may obtain access to written information about the service provider's policies and practices with respect to personal information, and
- the name or position name or title of a contact person who is able to answer on behalf of the service provider the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.

Questions about this Policy

If you have any questions with respect to our policies concerning the handling of confidential and personal information or your obligations under this Policy, please contact the CPO/COO at **rolson@tcet.com**

Approved by the Board of Directors on February 8, 2018