Procedure Statement:
The Flower Cart will have in place a procedure to mitigate damages and risk in the event of a breach of confidential information, including a privacy breach, a privacy incident, or a data breach.

Definitions:
Authorized – having official permission or approval

Confidential Information - all business or technical information, whether it is received, accessed, or viewed in writing, visually, electronically, or orally; Technical information; marketing and business plans; databases; specifications; formulations; tooling; prototypes; sketches; models; drawings; specifications; samples; computer software; forecasts; identity of, or details about, actual or potential customers or projects; techniques; inventions; discoveries; know-how; and trade secrets; business or technical information of any third party that The Flower Cart is in possession of.

Data Breach – an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. These may involve personal health information, personally identifiable information, trade secrets, or intellectual property.

Intellectual Property - Intellectual property is the legal right to ideas, inventions, and creations. It also covers symbols, names, images, designs, and models used in business.

Personal Information - Recorded information about an identifiable individual that may include his or her name, address, email address, phone number, race, nationality, ethnicity, origin, color, religious or political beliefs or associations, age, sex, sexual orientation, marital status, family status, identifying number, code, symbol, fingerprints, blood type, inherited characteristics, health care history including information on physical/intellectual disability, educational, financial, criminal, employment history.

Privacy Breach – Occurs when there is unauthorized access to, or collection, use, or disclosure of personal information. Such activity is unauthorized if it occurs in contravention in applicable privacy legislation such as the Personal Information Protection and Electronic Documents Act (PIPEDA) or similar provincial privacy legislation.

Privacy Incident – includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Trade Secrets - A trade secret is a formula or recipe, a practice, a process or standard operating procedure, a design, an instrument, a pattern, or a compilation of information. Trade secrets are not generally known or reasonably ascertainable by others. A business or individual can obtain an economic advantage over competitors or customers by using this information without authorization.

Unauthorized – Not having official permission or approval

Procedure:
In the event of a privacy breach the recommended protocol has 5 steps. Step 1 is the responsibility of the individual(s) who first become aware of the potential breach. Steps 2-5 are the responsibility of the Executive Director, working in cooperation with supervisors and staff as necessary.

Step 1: Reporting the Breach
Any employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of The Flower Cart will immediately inform his or her supervisor. The supervisor will inform the Executive

Director and will verify the circumstances of the possible breach. As soon as the breach has been confirmed to have or have not occurred, the supervisor will inform the Executive Director. This confirmation will occur within 24 hours of the initial report. When the breach has been confirmed, the Executive Director will implement the remaining four steps of the breach incident protocol.

Step 2: Containing the Breach

The Executive Director will take the following steps to limit the scope and effect of the breach. These steps will include:

1. Working with departments to immediately contain the breach; for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, or correcting weaknesses in security.
2. In consultation with the Board and/or The Flower Cart's lawyer, notify the police if the breach involves, or may involve, any criminal activity.

Step 3: Evaluating the Risks Associated with the Breach

To determine what others steps are immediately necessary, the Executive Director, working with supervisors and other staff as necessary, will assess the risks associated with the breach. The following factors will be among those considered in assessing the risks:

1. Personal Information Involved
    a. What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Health information, social insurance numbers, and financial information that could be used for identity theft are examples of sensitive personal information.
    b. What possible use is there for the personal information? Can the information be used for fraudulent or other harmful reasons?
2. Cause and Extent of the Breach
    a. What is the cause of the breach?
    b. Is there a risk of ongoing or further exposure of the information?
    c. What was the extent of the unauthorized collection, use, or disclosure, including the number of likely recipients and the risk of further access, use, or disclosure?
    d. Is the information encrypted or not otherwise readily assessable?
    e. What steps have already been taken to minimize the harm?
3. Individuals Affected by the Breach
    a. How many individuals are affected by the breach?
    b. Who was affected by the breach: employees, students, retirees, public, contractors, clients, service providers, participants, other individuals/organizations?
4. Foreseeable Harm from the Breach
    a. Is there any relationship between the unauthorized recipients and the data subject?
    b. What harm to the individuals will result from the breach? Harm may include:
        i. Security risk, (e.g. physical safety)
        ii. Identity theft or fraud
        iii. Loss of business or employment opportunities
        iv. Hurt, humiliation, damage to reputation or relationships
    c. What harm could result to The Flower Cart as a result of the breach? For example:
        i. Loss of trust in The Flower Cart
        ii. Loss of assets
        iii. Financial exposure
    d. What harm could result to the public? For example:
        i. Risk to public health
        ii. Risk to public safety

Step 4: Notification

Notification can be important mitigation strategy in the right circumstances. The key consideration overall in deciding whether to notify will be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used, or disclosed. The Executive Director will work with the appropriate supervisors and staff to decide the best approach to notification.

1. Notifying Affected Individuals
   Some considerations in determining whether to notify affected individuals include:
   a. Contractual obligations required notification.
   b. There is a risk of identity theft or fraud (usually because of the type of information lost, such as SIN, banking information, identical numbers).
   c. There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment).
   d. There is a risk of hurt, humiliation, or damage to reputation (for example, when the information lost includes medical or disciplinary information).
2. When and How to Notify
   a. When: Notification of individuals affected by the breach will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted these authorities will assist in determining whether notification will be delayed in order to not impede a criminal investigation.
   b. How: The preferred method of notification is direct – by phone, letter, or in person – to affected individuals. In direct notification – website information, posted notices, media – will generally occur only where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of communication in certain situations may be the most effective.
3. What will be Included in the Notification?
   Notification will include the following pieces of information:
   a. Date of the breach
   b. Description of the breach
   c. Description of the information inappropriately accessed, collected, used, or disclosed.
   d. The steps taken to mitigate the harm.
   e. Next steps planned and any long term plans to prevent future breaches.
   f. Steps the individual can take to further mitigate the risk of harm.
   g. Contact information for the Executive Director.
4. Others to contact
   Regardless of what obligations are identified with respect to notifying individuals, notifying the following authorities or organizations will also be considered:
   a. Police: if theft or other crime is suspected.
   b. Insurers or others: if required by contractual obligations.
   c. Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.
   d. The Board of Directors: the following factors are relevant in deciding to report a breach to the Board:
      i. The sensitivity of the personal information;
      ii. Whether the disclosed information can be used to commit identity theft
      iii. Whether there is reasonable chance of harm including non-pecuniary losses;
      iv. The number of people affected by the breach;
      v. Whether the information was fully recovered without further disclosure.

Step 5: Prevention/Learning

Once the immediate steps are taken to mitigate the risks associated with the breach, the Executive Director will investigate the cause of the breach. If necessary, this will include a security audit, as well as physical, organizational, and technological measures. As a result of this evaluation, the Executive Director will assist the responsible supervisors to put into effect adequate long term safeguards against further breaches. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. The resulting plan will also include audit recommendations, if appropriate.

Related Information:

Contact:
Executive Director

Roles and Responsibilities:
Employee
- Notify their supervisor in the event of a perceived privacy breach.
- Work with the Executive Director, legal counsel, the external IT team, and/or the RCMP in the event of an investigation.

Supervisor
- Notify the Executive Director of a perceived privacy breach.
- Work with the Executive Director, legal counsel, and/or the RCMP in the event of an investigation.

Executive Director
- Steps 2 - 5

External IT Team
- Contacted in the event of a technological breach.

Revision History: