Privacy, Confidentiality, Protection of Information, Privacy Breach Protocol

Policy

Agilec respects the privacy of our clients, customers, and employees. We are committed to handling all personal information in keeping with the Personal Information Protection and Electronics Document Act (PIPEDA), and the ten privacy principles.

We enact this policy by following our Privacy Practices.

Responsibility

Agilec has appointed a Privacy Officer who is responsible for establishing and implementing our privacy policy and practices.

Privacy Officer:
Brian Martin
905 443 1001 ext. 2300
bmartin@agilec.ca

The full responsibilities of the Privacy Officer are detailed in the Accountability section of our Privacy Practices.

The Privacy Officer is supported by a Privacy Team consisting of each Agilec Team Leader. The Privacy Team is responsible for conducting local team privacy training, monitoring local application of Agilec privacy practices, and ensuring that privacy issues encountered at a local level are communicated to the Privacy Officer.

Every Agilec employee is responsible for the consistent application of our privacy practices. Employees also adhere to the Vocational Rehabilitation Association of Canada Code of Ethics, which contains principles for the ethical handling of client personal information.

Privacy Practices

Introduction
We understand the importance of protecting the personal information we gather from customers. We are committed to collecting, using, disclosing, and retaining personal information responsibly. We endeavour to be as open and transparent as possible about the way we handle personal information. To ensure the thoroughness and completeness of our Privacy Practices, we have organized them according to the ten privacy principles.

Principle 1: Accountability
Agilec understands and accepts our responsibility for the personal information we collect directly or receive from other sources in the course of business activity.

A Privacy Officer has been designated by Agilec to oversee our approach to privacy and ensure compliance with PIPEDA and our privacy practices. This includes:

- Tracking data concerning our privacy practices, such as number of enquiries, requests, complaints, breaches, etc.
- Assessing the effectiveness of the system as well as the effectiveness of improvements to the system.
- Reviewing Agilec privacy practices, and ensuring they remain current with changes to applicable legislation and the environment (including information technology).

Details about how we monitor our adherence to privacy law and our practices are contained in our Privacy Compliance Framework.

In Practice: Agilec is accountable for all Personal Information in our possession, including any stored on employee U: drives. To help us fulfill our obligations:

- Keep the amount of candidate information you store on your U: drive to a minimum.
- Create a dedicated folder ("Candidate Information") and keep any/all candidate information you store on your U: drive within this folder.
- Delete candidate information from your U: drive when it is no longer needed.

Keep in mind that candidates are entitled to access all personal information that Agilec has about them, including any that is stored on your U: drive.

Agilec recognizes that our privacy responsibility extends to include personal information that has been transferred to a third party. We use contractual or other means to provide a comparable level of protection for information that is being accessed and/or processed by third parties.

Principle 2: Identifying Purposes for Collecting Information
Before collecting any personal information, Agilec will always be clear with ourselves and our clients/customers about why we are doing so.

In order to fulfill this principle:

- We will ensure that employees who collect personal information are able to clearly explain why they are doing so and how the information will be used.
- Any forms we use to collect personal information will include a description of the purposes for collection.
- In order to avoid collecting information we do not need, we will endeavor to be as specific as possible about our purposes for each piece of information we collect.
- If we know that personal information is going to be shared with others outside of Agilec, we will explain this at the time of collection.
- We will not use collected information for new purposes that we have not explained to the customer unless we obtain subsequent specific consent for the new purposes.

Principle 3: Consent
Agilec obtains informed consent for the collection, use, and disclosure of personal information, except where it might be inappropriate to obtain consent, and subject to some exceptions set out in law.

This principle requires that we explain our purposes for the information (in keeping with Principle 2) and that we are sure the individual clearly understands. To facilitate understanding, our explanations will use plain and concise language.

Consent may be given in a number of ways. In general, we apply the following guidelines which increase the rigor of the consent as the sensitivity, depth, or complexity of purpose for the information increases:

- Consent related to the most basic personal information (e.g., name and contact information that will not be shared outside Agilec) can be obtained verbally and need not be documented.

- Consent with respect to more detailed personal information that will be used exclusively inside Agilec can be obtained verbally. The fact that verbal informed consent was obtained must be noted within the case file.
- Consent concerning personal information that will be shared with third parties (including referring agencies) should be obtained in writing, usually via a signature on a formal consent form.

Consent must be renewed if the collection purpose or disclosure details change.

An individual may withdraw consent at any time. In these cases, we inform the individual about the possible implications of withdrawing consent.

Principle 4: Limiting Collection of Personal Information
Agilec collects only that information which is necessary for the purposes identified and communicated at the time of collection.

This means:
- We will be clear about our purposes before we collect information (see Principle 2).
- Our forms for obtaining information will be constructed to gather only the necessary information.
- We do not record/document non-essential personal information that comes up during conversations with customers.

In Practice: We must be careful not to collect information based on assumptions about where services might lead. For example, we should not obtain a candidate's SIN until we have determined that the individual is going to access services where the SIN is required information.

Principle 5: Limiting Use, Disclosure, and Retention
Agilec will not use or disclose personal information for purposes other than for which the information was collected, except with express consent or as permitted by law.

Use:

If we intend to use personal information for a purpose different than was identified at the time of collection, we must first obtain and document consent for the new purpose.

Disclosure/Release of Information (ROI):

Within Agilec
At the time of collection, we inform clients/customers that their personal information may be shared with other Agilec employees who have a role in accomplishing the identified purposes. This allows team leaders, finance, peers (for case conferencing or vacation coverage, for example), and others the access they need to perform their roles. However, personal information is not to be shared with, or accessed by, Agilec employees who need not be involved in a customer's case.

Outside Agilec
We will not disclose personal information to anyone outside Agilec unless the individual or organization receiving the information is specifically authorized via the written consent of the customer. This includes family members and others acting on behalf of an individual.

This practice applies to written, electronic, and verbal forms of disclosure.

Exceptions to Consent Requirements
PIPEDA contains a number of exceptions to the requirement that consent be obtained prior to disclosure. Situations involving these exceptions occur only rarely. The ones we are most likely to encounter at Agilec are:

- When we are required to comply with a warrant, court order, subpoena, or the law.
- When a government institution (e.g., the police) requests the information in order to enforce the law. (Note: In these cases, we usually require the police to obtain a warrant prior to our releasing the information to them.)
- When we have reasonable grounds to believe that the information relates to illegal activity, we can share it with enforcement officials without waiting for them to come to us.
- In an emergency that threatens the life, health, or security of an individual.

In Practice: In any of the above situations, a minimum of two Agilec leaders will be involved in the decision process. The Privacy Officer is consulted. If the Privacy Officer is not available to participate in decision making, the leaders involved are responsible to inform the Privacy Officer of the situation and the actions taken as soon as possible thereafter.

Retention and Destruction:

Retention of Personal Information
Agilec retains records containing personal information only as long as they are needed for service or contractual reasons, or as required by law. This practice applies to both electronic and hard copy (paper) records.

In Practice: Leadership for every Agilec project determines how long personal information shall be retained beyond the conclusion of services (the Retention Period). The needs of the Finance Department must be factored into this decision. The project Retention Period is communicated to the Privacy Officer who ensures alignment with our Privacy Practices and law, and monitors compliance.

Destruction of Personal Information
All Agilec records (paper and electronic) containing personal information shall be destroyed within one year of reaching the Retention Period.

Agilec has prepared a guide to the secure destruction of paper and electronic information.

In Practice: Leadership for every Agilec project must ensure that all personal information records that have passed the Retention Period are destroyed, at least annually, using the secure destruction methods described in the guide.

Principle 6: Accuracy of Personal Information
Agilec takes steps to ensure that customer personal information is as accurate, complete, and as up-to-date as needed for the purposes that it is to be used. Our intent is to eliminate the use of inaccurate information in making service recommendations or decisions.

In Practice: During meetings with customers, employees ask whether any personal information has changed, and update the information accordingly.

Principle 7: Safeguards for Personal Information
Agilec will take appropriate measures to safeguard personal information from unauthorized access, disclosure, use, or tampering. Safeguards shall be appropriate for the sensitivity of the information being protected.

We have established a set of organizational, physical, and technological methods to protect personal information. It is the responsibility of every Agilec

employee to be familiar with these methods and to ensure that customer personal information is safeguarded at all times, whether recorded on paper or electronically.

Organizational Safeguards

- Agilec employees, students, and third party service providers sign confidentiality agreements binding them to safeguard personal information to which they have access.
- New employees are trained on Agilec's privacy practices as part of our onboarding process.
- All employees receive privacy refresher training annually.
- Privacy inspections or audits are conducted quarterly under the guidance of the Privacy Officer.
- The Privacy Officer conducts an annual review of Agilec's privacy program. The approach may include:
    - Evaluation and updating of our Privacy Policy and practices;
    - Review of our experience over the past year (including any privacy complaints or breaches);
    - Comparisons to best practices inside or outside Agilec;
    - Evaluation against changes in legislation or customer requirements;
    - Feedback from service delivery teams; and/or
    - Assessment of internal compliance and/or employee knowledge.

Physical Safeguards

- Documents printed on a shared printer must not be left in the view of unauthorized persons.

In Practice: Options include:

- Picking up documents immediately upon printing
- Sending print jobs to a secure mailbox, to be printed when the authorized employee enters their personal code at the printer
- Having an authorized peer at the printer to retrieve the documents as they are printed

- Each employee must ensure documents are not left in the view of unauthorized persons.
- Cabinets containing personal information must be in non-public areas or be kept locked. All cabinets must be locked whenever the office is vacated.
- Agilec provides separate fax machines for public/customer and employee use. Employee fax machines must be located in non-public areas. Incoming faxes must be retrieved and distributed to the addressees regularly.
- Each Agilec facility has locking doors and electronic security protection equipment installed at each external entrance. Only Agilec employees

and authorized third parties are issued entrance keys and codes. Keys are tracked and recovered from employees/third parties that no longer require them, and security codes are changed at the same time.
- Each area where personal information is stored is secured with an entrance lock and/or locking cabinets. A key is issued to a designated person responsible for the security of that area. One duplicate key exists, and is secured by the local Team Leader or designate.

> **In Practice:** We remind candidates to protect their information while making use of our resources (for example, by posting instructions not to save files to our computers and to pick up documents from the printer immediately).

Technological Safeguards

Computers:

- Agilec maintains a secure Virtual Private Network.
- Additional information about computer security, including:
  - Passwords
  - Screen lock
  - Saving and accessing information
  - Laptop and other portable computer security
  - Smart phones

  is contained in the *Security of Technology and Information* section of Agilec's Technology Practices.

Transmission Safeguards

There are a number of options available for Agilec employees to use to transfer Personal Information to others. Each method has its own privacy considerations.

Customer Portal:

- In some instances, Agilec provides a web-based portal for the secure two-way exchange of SSL-protected information between Agilec and second or third parties.

Email - Internal:

- Internally, Agilec's VPN and secure server ensure that all email messages and attachments sent between Agilec email addresses are secure.

Email – External:

- Any email sent to an address outside Agilec must be considered **unsecure**, because the contents of the email and any attachments can be viewed along the way by any network the message passes through.
- At Agilec, we recognize that:

- Not all personal information carries the same level of sensitivity.
- Most members of the public are comfortable using email to send non-sensitive personal information.
- Email is often the most efficient and time-effective way to exchange information between parties.

Therefore, Agilec's privacy practices allow for emailing *non-sensitive personal information* externally, under the following conditions:

Requirements:

1. Every candidate reads or has explained to them Agilec's email practices using our Protecting Your Privacy document.
2. The candidate's agreement or disagreement with respect to our email practices for their personal information is obtained and recorded in CTS.
3. The sensitivity of the personal information sent by email is low, in keeping with the following chart:

Emailing permitted [1]	**Emailing prohibited**[2]
Resumes	Medical information
Cover Letters	Reports (Progress, Assessment, etc.)
Schedules	Program applications (e.g., SC, OSEB)
Appointments	Names combined with other ID numbers
Pay stubs/earnings (if no SIN included)	SIN
Referrals (if information sensitivity is not greater than resume)	Referrals (if they contain sensitive information beyond what would be in a resume, e.g., disability)
Academic info (with name or ID# only, not both)	TIPAs
CTS Action Plans	Driver's Abstract
Job Postings/employer contact info	Criminal Reference checks
Satisfaction surveys and responses	

[1]Password protection not necessary [2]See password protection below
[3]These lists are not exhaustive. Use the content as a guide to evaluate other forms of personal information before sending by email.

In Practice: As a safeguard against breaches that occur when a message is inadvertently sent to one or more wrong addressees, it is best to avoid including personal identifying information in any email whenever possible (including internal email). For example, individuals can be referenced by use of an Agilec-assigned number or code that would be meaningless to anyone outside Agilec.

- Password Protection: This approach provides limited, unreliable protection against malicious access to personal information. Therefore, it is no longer part of Agilec's standard email practices. However, in exceptional cases

where email is the only available option to transmit sensitive personal information (see the *emailing prohibited* list above), the information may be sent as a password-protected attachment to an unsecure email. No identifiable personal information should be in the title or body of the email itself. Exceptions should never be made for highly sensitive information. How to Password Protect a Document or a PDF.

> **In Practice:** Password protection is a barrier to humans as well as to automated 'sniffers' that scan Email and attachments for key types of content. Passwords create an envelope that must be opened to view or sniff the document. However, password-busting software is capable of breaking most passwords.
>
> When password protection is not available, printing and scanning a document to PDF format changes the text content into a picture that cannot be sniffed (although it can still be viewed by humans).

- When a customer's Email privacy requirements differ from these practices, the more restrictive of the two shall be followed.

Customer hand delivery:

- An Agilec customer can be used to deliver, obtain, or return documents containing their own personal information. While this can shield Agilec from full responsibility should the information go astray, we may still be deemed to be party to any breach. The reliability of the customer, the time sensitivity, and the nature of the personal information should all be considered before using this option.

> **In Practice:** This approach can be effective when attempting to obtain information from physicians.

Courier:

- Generally secure (shipment is sealed, and can be tracked).
- Offer guaranteed delivery timeframes.
- May be impractical and/or cost-prohibitive.
- Use pre-printed address and return address labels to lessen risk of delivery to an incorrect address.

Express Post:

- Similar to courier.
- Can pay a fee to request a signature upon delivery to enhance tracking, however this can cause a delayed delivery and some inconvenience for the recipient.

Regular Mail:

- May be used to deliver non-sensitive documents to the customer.
- Do not use regular mail to deliver documents containing medical, disability, financial, or other confidential personal information such as Social Insurance Number (SIN).
- Use pre-printed address and return address labels to lessen risk of delivery to an incorrect address.

Personal delivery by Agilec employees:

- Not recommended.
- Requires heightened care and diligence on the part of the employee.
- Minimize stops along the way.
- Employees must keep information in a locked briefcase which is kept with their person or in a locked vehicle trunk at all times.

In Practice: Agilec field employees should take only the minimum information/number of files needed for the day to lessen the potential of unauthorized access or exposure.

Faxing:

- This approach has inherent risks: sending to incorrect recipient; receiving fax is not secure.
- Use pre-programmed fax numbers in the fax machine to lessen risk of mis-dialing a number.
- Call ahead of transmission to confirm an authorized receiver is aware of incoming fax.
- Arrange for confirmation of fax receipt by the authorized receiver.

Telephone:

- Take steps to satisfy ourselves that the individual we are speaking with is covered by the customer's consent to disclose.

External Referrals:

- Use standardized Agilec referral forms to limit the customer information we share to what we have determined is necessary for the referred services.

Principle 8: Openness about Privacy

Agilec makes information about our privacy practices readily available to our customers in a variety of ways, including:

- Publically posting a summary of our policy and practices and the contact information for the Agilec Privacy Officer at all Agilec locations.

- Using customer consent forms that explain how Agilec collects, uses, and discloses personal information.
- Making our Agilec Privacy Policy and Practice document available on our website or upon request.

Principle 9: Customer Access to Personal Information
Upon written request and with reasonable notice, Agilec will inform a customer of the existence of any of his/her personal information in our possession, and will provide access to that information.

If requested, Agilec will also provide an accounting of how the customer's personal information has been used, including third party disclosures. In providing this information, we will attempt to be as specific as possible.

We will respond to requests for access within a reasonable period of time, and at minimal or no cost to the customer. The requested information will be made available in a format that is generally understandable.

A customer is free to challenge the accuracy and completeness of their information and seek to have it altered, amended, or changed.

> **In Practice:** Additional details concerning how to respond to requests for personal information are contained in our File Access Guidelines.

Principle 10: Challenging Compliance
A customer or an employee may challenge our compliance with these principles by using the Agilec Formal Complaint Process. Information concerning the Complaint Process is available on the Agilec website or at any Agilec location. Agilec employees will help those who wish to raise a privacy concern to access the Complaint Process.

All formal privacy-related complaints are addressed by the Agilec Privacy Officer, who will also inform the complainant of other avenues of recourse available to them such as contacting the Privacy Commissioners of Ontario or Canada. Should it be determined that a complaint is justified, the Privacy Officer will take appropriate measures, including, if necessary, amending any Agilec practices.

QA Approach to Privacy

Quarterly internal inspections or audits of our compliance with the Agilec Privacy Policy and Practices are conducted under the direction of the VP Quality Assurance.

In addition to ongoing evaluation of compliance, in order to ensure the ongoing effectiveness and improvement of the Privacy System, the Privacy Officer leads an annual review of the system, and reports on the results.

Additional details are contained in our Privacy Compliance Framework.