

WCG International Consultants Limited

Personal Information Protection Policy

At WCG International Consultants Limited (“WCG”), we are committed to protecting the personal information of our employees, our clients and those who participate in the programs we offer. Providing our various services involves the collection, use and disclosure of certain personal information; protecting that personal information is one of our highest priorities.

While we have always respected the privacy of our employees, clients and program participants and safeguarded their personal information, we have strengthened our commitment to protecting personal information as a result of British Columbia’s *Personal Information Protection Act* (PIPA). This law sets out the ground rules for how B.C. businesses and not-for-profit organizations may collect, use and disclose personal information. In the case of the personal information of our program participants, it is safeguarded under Part 3 of the *Freedom of Information and Protection of Privacy Act*.

We will inform our clients and employees of why and how we collect, use and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Personal Information Protection Policy, in compliance with PIPA, outlines the principles and practices we will follow in protecting the personal information of our clients and employees. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of their personal information and allowing them to request access to, and correction of, their personal information.

Scope of this Policy

This Personal Information Protection Policy applies to WCG and its subsidiaries. It also applies to all contractors who provide any service to WCG and engage in collecting, using or disclosing personal information on behalf of WCG or its subsidiaries.

This Policy does not apply to the personal information that WCG may possess under contracts that involve program participants in the BC Employment Program or the BC Employment Program for Persons with Disabilities. Any such information is under the control of the Ministry of

Employment and Income Assistance and therefore subject to the protections provided under the *Freedom of Information and Protection of Privacy Act*.

Definitions

Personal Information – means information about an identifiable individual. For example, WCG collects the name, age, home address and phone number, social insurance number, education, and employment information of its employees and uses this personal information to manage the employment relationship. Personal information does not include contact information or work product information (described below).

Contact Information – means information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or PIPA.

Work Product Information – means information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the personal information.

Privacy Officer – means the individual designated responsibility for ensuring that WCG complies with this policy and PIPA.

Program Participant – means an individual who is a client of the BC Employment Program or the BC Employment Program for Persons with Disabilities.

Policy 1 – Collecting Personal Information

1.1 Unless the purposes for collecting personal information are obvious and the employee or client voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

1.2 We will only collect employee or client information that is necessary to fulfill the following purposes:

- To verify identity;
- To verify creditworthiness;
- To identify client preferences;
- To meet regulatory requirements.

Policy 2 – Consent

- 2.1 We will obtain the consent of employees and clients in order to collect, use or disclose their personal information (except where, as noted below, we are authorized to do so without consent).
- 2.2 Consent can be provided orally, in writing, or electronically or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the employee or client voluntarily provides personal information for that purpose.
- 2.3 Consent may also be implied where an employee or client is given notice and a reasonable opportunity to opt out of his or her personal information being used for mail-outs, the marketing of new services or products, fundraising and the client does not opt out.
- 2.4 Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), employees or clients can withhold or withdraw their consent for WCG to use their personal information in certain ways. A client's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service. If so, we will explain the situation to assist them in making the decision.
- 2.5 We may collect, use or disclose personal information without the consent of the employee or client in the following circumstances:
- When the collection, use or disclosure of personal information is permitted or required by law;
 - In an emergency that threatens an individual's life, health, or personal security;
 - When the personal information is available from a public source (e.g., a telephone directory);
 - When we require legal advice from a lawyer;
 - For the purposes of collecting a debt;

- To protect ourselves from fraud;
- To investigate an anticipated breach of an agreement or a contravention of law.

Policy 3 – Using and Disclosing Personal Information

3.1 We will only use or disclose the personal information of employees or clients where necessary to fulfill the purposes identified at the time of collection or for a purpose reasonably related to those purposes such as:

- To conduct client surveys in order to enhance the provision of our services;
- To contact our clients directly about products and services that may be of interest;

3.2 We will not use or disclose the personal information of employees or clients for any additional purpose unless we obtain their consent to do so.

3.3 We will not sell any personal information to other parties.

Policy 4 – Retaining Personal Information

4.1 If we use the personal information of employees or clients to make a decision that directly affects them, we will retain that personal information for at least one year so that they have a reasonable opportunity to request access to it.

4.2 Subject to policy 4.1, we will retain the personal information of employees or clients only as long as necessary to fulfill the identified purposes or a legal or business purpose.

Policy 5 – Ensuring Accuracy of Personal Information

5.1 We will make reasonable efforts to ensure that the personal information of employees and clients is accurate and complete where it may be used to make a decision about them or is disclosed to another organization.

5.2 Employees or clients may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought. A request to correct personal information should be forwarded to the Privacy Officer.

5.3 If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to

which we disclosed the personal information in the previous year. If the correction is not made, we will note the correction request of the employee or client in the file.

Policy 6 – Securing Personal Information

6.1 We are committed to ensuring the security of the personal information of employees and clients in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

6.2 The following security measures will be followed to ensure that personal information is appropriately protected:

- the use of locked filing cabinets;
- physically securing offices where personal information is held;
- the use of user IDs, passwords, encryption, and firewalls;
- restricting employee access to personal information as appropriate (i.e., only those that need to know will have access);
- requiring by contract that any service providers provide comparable security measures.

6.3 We will use appropriate security measures when destroying the personal information of employees and clients, such as shredding documents, and deleting electronically stored information.

6.4 We will continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

Policy 7 – Providing Employees and Clients with Access to Personal Information

7.1 Employees and clients have a right to access their personal information, subject to the limited exceptions found in section 23 of the *Personal Information Protection Act* pertaining to such matters as solicitor-client privilege, disclosure that would reveal the personal information about another individual, and health and safety concerns.

7.2 A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. A request to access personal information should be forwarded to the Privacy Officer.

- 7.3 Upon request, we will also tell employees and clients how we use their personal information and to whom it has been disclosed if applicable.
- 7.4 We will make the requested information available within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.
- 7.5 A minimal fee may be charged to clients for providing access to their personal information. Where a fee may apply, we will inform the client of the cost and request further direction from them on whether or not we should proceed with the request.
- 7.6 If a request is refused in full or in part, we will notify the employee or client in writing, providing the reasons for refusal and the recourse available to them.

Policy 8 – Questions and Complaints: The Role of the Privacy Officer or designated individual

- 8.1 The Privacy Officer is responsible for ensuring WCG's compliance with this Policy and the *Personal Information Protection Act*.
- 8.2 Employees and clients should direct any complaints, concerns or questions regarding WCG's compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the employee or client may also write to the Information and Privacy Commissioner of British Columbia.

Contact information for WCG's Privacy Officer:

David Shaw
Chief Privacy Officer
WCG International
Third Floor
915 Fort Street
Victoria BC
V8V 3K3
toll free: 1-888- 562-9283
fax: 250-389-0696

- 8.3 Program Participants who may have concerns about the protection of their personal information or who may want to request access to records in the custody or under the

control of the Ministry of Employment and Income assistance may wish to contact the
Ministry at the following address:

Director, Information, Privacy and Records Services

Ministry of Employment and Income Assistance,

PO Box 9972 Stn Prov. Govt.

Victoria BC

V8W 9R5

Tel: (250) 387-3128

Fax: (250) 387-3311