Insights West Privacy Policy

Insights West confirms that we operate in full compliance with FIPPA and with the restrictions on storing, accessing, or disclosing personal information outside Canada.

Following is a summary of our privacy policy.

RESPONDENT/PARTICIPANT PRIVACY

When Insights West conducts research, our invitations and questionnaires clearly identify our company and explain the purpose(s) of our contact. We contact participants for the following purposes:

- To invite people to participate in survey, focus group, or interview research;
- To validate answers given in a recent survey, focus group, or interview that we conducted;
- To provide services and support that participants have requested;
- To notify participants if they have won a prize draw that we sponsored; and
- To fulfill incentives for participation.

When participants take part in Insights West research, we may ask them for personal opinions, as well as sometimes personal information, such as age, gender, residence (city and sometimes postal code), and household composition. We ask these questions to help ensure that the demographic profiles of individuals who participate in our surveys accurately reflect the target population. Personal information is also used when needed to examine results by demographic variables during the data processing stage (in aggregate form only).

Insights West always collects personal information by fair and lawful means. We collect personal information where we have obtained participant consent to do so or as otherwise permitted by law. Participation is completely voluntary. Participants are always free to choose not to answer questions or to discontinue participation at any time.

For research conducted online, it is possible to turn on or off the tracking of IP addresses (typically used to ensure no duplicate data from the same person). If no personal information is collected in the survey, without an IP address collected, there would be no way to link response to any individual, providing complete anonymity and confidentiality.

All survey responses in a given survey are combined with the responses of all other respondents. The results are reported in aggregate form only. We will never intentionally report an individual's survey responses.

Suite 304, 1140 Homer Street
Vancouver, BC
V6B 2X6
778-891-4762

www.insightswest.com
www.yourinsights.ca

The only exception when we may disclose personal information or survey responses is when participants consent to sharing their personal information and individual responses with the third parties for a specified purpose. Insights West always explains the reason for the disclosure to the respondent and obtains express permission from the respondent before making any such disclosure.

In addition to keeping survey responses confidential, we will never sell, share, rent, or otherwise intentionally transfer personal information to anyone else (unless there is explicit consent as described above). As well, we will never try to sell participants anything.

STORAGE AND ACCESS TO PERSONAL INFORMATION

- Only those staff directly involved in work for an individual client have access to the project files. Insights West can apply password protection to individual files and folders as needed to ensure the security of all documents and data related to projects. At the beginning of our work with a client, these settings are implemented and updated on an as-needed basis. Those who have access to project folders are not able to share access with anyone else.
- Secure passwords for file storage and email accounts are generated by the Office 365 environment and can only be changed by our Office 365 administrator, Allan Dawe, who has an additional level of security applied to his account through two-factor authentication. If 5 unsuccessful login attempts are made the system will automatically lockout the account for 30 minutes.
- As noted above under respondent /participant privacy, no personally identifying information (such as name, address, telephone number) of respondents is ever provided to a client unless the respondent has explicitly given their consent to do so.

TRANSFER OF INFORMATION

Information that needs to be transferred to sub-contractors, other staff or clients is done so via email. To ensure that communications remain secure, we have the ability to encrypt emails and add digital signatures.

- All personal/confidential information is removed from data files prior to transfer to any outside parties.
- Where possible, data transmissions from mobile devices are encrypted.
- Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device is disabled when not in use to prevent unauthorized wireless access to the device.

- Where available, wireless access is configured to query the user for confirmation before connecting to wireless networks. For example, when Bluetooth is on, select the "check with me before connecting" option to prevent automatic connections with other devices.

PROCESS FOR DESTROYING SENSITIVE INFORMATION

Once a study is complete, project managers overwrite all sensitive information, replacing it with non-sensitive and non-identifiable data. All emails containing personal information relating to each study is deleted from the internal memory of Insights West employees' laptops as well as from our server.

Any printed materials produced internally are shredded and disposed of regularly using the professional services of Shred-it shredding services.

MOBILE COMPUTING DEVICE POLICY

Mobile computing devices are devices such as tablets, smartphones, e-readers, and laptop computers. The very features that make these devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to Insights West when they contain customer or other confidential data. Major features of mobile devices that cause a risk to the user and potentially Insights West include their small size (they can be easily lost, stolen, or misplaced); weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of interconnectedness.

Specific features of the policy:

- Employees are instructed to keep their mobile devices with them at all times or store them in a secured location when not in use. They are told not to leave their mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.)
- Mobile devices are password protected and auto lockout enabled. The password should block all access to the device until a valid password is enabled. The password used should be as strong a password as the device will support.
- "Remote wipe" features, if available, are enabled. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.
- Employees are instructed not to circumvent security features or otherwise "jailbreak" the mobile device.

- All standard security protocols are followed, including ensuring the device has current anti-virus software and all operating system and application updates and patches. Firewalls are enabled if possible.
- All mobile devices are wiped /all data is securely deleted data before disposing of it.
- Employees are instructed to immediately report lost, stolen, or misplaced mobile devices to the police. If the mobile device contained Insights West data, employees must also inform the Insights West management team about the lost, stolen, or misplaced device.

If you have any privacy questions or concerns about Insights West's Privacy Policy, please contact us by e-mail at info@insightswest.com, by phone at 778-379-1140 or by mail at Suite 304-1140 Homer Street, Vancouver, BC, V6B 2X6.