INDEPDENDENT PURCHASING COOPERATIVE
PRIVACY POLICY

Independent Purchasing Cooperative, Inc.
9200 South Dadeland Boulevard, Suite 800
Miami, Florida 33156
Telephone: 1-888-445-9239
Technical Support: webmaster@ipcoop.com

Scope of This Privacy Policy

Independent Purchasing Cooperative, Inc. ("IPC") is the host of and manages www.ipcoop.com, www.profitpulse.ipcoop.com, and www.mysubwaycareer.com (together, the "Websites"). IPC is an independent non-profit purchasing cooperative which is owned by and provides services to Subway® Franchisees around the world (the "Subway® Franchisees").

This Privacy Policy discloses how IPC collects, protects, uses, and shares Personal Information gathered about you. The term "Personal Information" means any information concerning an identified or identifiable individual. IPC shares such information with its wholly-owned subsidiaries and other Subway®-related entities and service providers for the purpose of furthering the business of the Subway® line of restaurants (the "Subway® Restaurants").

IPC's privacy practices are consistent with U.S. law, Canada's Personal Information Protection and Electronic Documents Act, and other applicable law, including the European Union's General Data Protection Regulation ("GDPR"), which governs the collection, storage, use, and transfer of personal information for European Union residents. IPC also complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, as discussed below.

IPC acts as both a controller and processor of your Personal Information within the meaning of the GDPR. The legal bases for IPC's processing of your Personal Information is your general and express consent as detailed herein and IPC's pursuit of legitimate business interests.

Contact information for IPC and its designated data protection officer (the "Privacy Officer") are set forth below. If you have questions about this Privacy Policy or the protection of your information, please contact the Privacy Officer as set forth below.

General and Express Consent Regarding Information

A. General Consent. IPC respects the privacy of users of its Websites, visitors to the Subway® Restaurants, whether or not as customers, and Subway® Franchisees. IPC collects information in a fair and non-intrusive manner and recognizes the need for appropriate protections and management of the information that you provide. IPC has adopted, implemented, and conducts its business pursuant to this Privacy Policy in order to assist you in understanding what types of Personal Information IPC may collect, how that information may be used, and with whom the information may be shared. This Privacy Policy applies to all information gathered by or on behalf of IPC, whether in writing, verbally, or electronically, or through the Websites.

BY SUBMITTING PERSONAL INFORMATION TO IPC, AND/OR BY ACCESSING AND USING THE WEBSITES, YOU AGREE THAT IPC MAY COLLECT, STORE, USE, AND TRANSFER YOUR PERSONAL INFORMATION IN ACCORDANCE WITH THIS PRIVACY POLICY OR AS PERMITTED OR REQUIRED BY APPLICABLE LAW. IF YOU DO NOT CONSENT TO THE COLLECTION, STORAGE, USE, OR TRANSFER OF YOUR PERSONAL INFORMATION AS DESCRIBED IN THIS PRIVACY POLICY, YOU SHOULD NOT SUBMIT PERSONAL INFORMATION TO IPC OR ACCESS OR USE THE WEBSITES.

B. Consent to Share and Disclose Information. By submitting Personal Information to IPC, and or/by accessing and using the Websites, you expressly consent to IPC sharing your Personal Information as follows:

IPC shares Personal Information with the following Subway®-related entities and third-party agents or service providers who perform functions on our behalf:

(1) IPC's wholly-owned subsidiaries Value Pay Services LLC and PLXIS LLC;

(2) Subway® international purchasing cooperatives that are owned by Subway® Franchisees and which provide services to the Subway® Franchisees (the "Co-op Group");

(3) various Subway®-related including but not limited to Doctor's Associates LLC ("DAL"), Subway Franchise Systems of Canada, ULC, Subway IP LLC, FWH Technologies, LLC, and Franchise World Headquarters, LLC (the "Subway® Group"); and

(4) Subway® Group advertising entities that are members of the Subway Franchisee Advertising Fund Trust (the "FAF Group").

All of these entities are "Third Parties".

In addition, IPC may also share Personal Information with companies that provide support services to it, such as credit card processors, mailing houses, web hosts, technical support providers, fulfilment centers, or other service providers, as well as companies involved in enforcing or investigating transactions or business operations, because these companies may need information about you in order to perform their functions. IPC limits the use of information shared with these companies to the purpose for which IPC hired them, but IPC does not control these companies. These companies are "Service Providers". In this policy, both Third Parties and Service Providers are "Recipients".

C. Consent to International Data Transfers. IPC and the Recipients are multi-national entities with operations throughout the world. In order for those entities to be able to provide you with suitable goods, services, and promotions, you expressly consent to your Personal Information being transferred and disclosed internationally, including within and outside the U.S., Canada, and the European Union. Some of these jurisdictions may have laws that provide less protection to your Personal Information than you receive under the laws in our own jurisdiction. The U.S., for instance, has not received a decision from the European Commission determining that it provides adequate protection to Personal Information. Canada, by contrast, has received such a decision. IPC will take reasonable steps to ensure that any transfer or disclosure of Personal Information to or within any jurisdiction is in compliance with applicable law and receives the level of protection required by the Privacy Shield Framework referenced above and the GDPR. Such steps will include reliance upon the Privacy Shield certification process, other similar processes where applicable, and/or GDPR-compliant data transfer agreements incorporating approved standard contractual clauses for the protection of Personal Information. You can obtain additional details regarding those safeguards by contacting IPC's Privacy Officer, as set forth below.

D. Consent to Electronic Notice If There is a Security Breach. If IPC or a Recipient is required to or wishes to provide notice of unauthorized access of their data security systems or unauthorized or unlawful access to or processing of your Personal Information, you agree that IPC and/or the Recipient may do so by posting notice on the Websites or sending notice to any email address which IPC or the Recipient has for you.

E. Right to Withdraw Consent. You have the right to withdraw your consent to IPC's collection, storage, use, and transfer of your Personal Information at any time. You also have the right to request that IPC provide you with access to, correct, delete, or restrict the processing of your Personal Information. If you wish to exercise any of those rights, please contact the IPC Privacy Officer as set forth below.

Collection and Use of Personal Information

IPC collects and uses your Personal Information in a fair and non-intrusive manner, as set forth in this section. If IPC intends to materially change the manner in which it collects and/or uses your Personal Information, it will notify you by email or by means of a notice on the Websites describing the material changes. IPC will also update this Privacy Policy accordingly, as set forth below. Your continued submission of Personal Information and/or use of the Websites after notification of such changes shall constitute your agreement to be bound by such changes.

A. Personal Information Collected in Connection With Online Purchases, Registration, Support, and Use of Subway® Cards. Other Subway®-related entities and service providers collect Personal Information in connection with online purchases, registration, support, and use of Subway® Cards. The Personal Information collected includes name, email address, birthdate, gender, mobile phone number, Subway® Card and PIN numbers, and credit card information, as well as billing and shipping addresses, transactional information, and other unique user identifiers. Some of this information is shared with IPC and its wholly-owned subsidiary VPS in connection with VPS' role as administrator of the Subway® Card program. VPS also collects some of the foregoing information directly when processing special orders for Subway® Cards with Braille text and providing support for Subway® Cards with Braille text.

B. Personal Information Collected on the Websites. Personal Information collected on the Websites includes email address. IPC shares this information with the Co-op Group, the Subway® Group, and the FAF Group for marketing purposes if you elect to receive communications.

C. Other Details Relating to Website Use.

User Name and Password. IPC requires that you create a username and password in order to access the Member or non-public pages on the Websites. IPC does not divulge usernames or passwords to anyone. Should you need to change or remove your username or password, contact the IPC Privacy Officer as set out below.

Email & Mobile Updates. You may have the opportunity to elect to receive email and mobile communications from IPC and the FAF Group. IPC and the FAF Group will only email you or send you mobile messages or alerts if you elect to receive such communications. If you elect to receive such communications, IPC and the FAF Group will send you occasional updates about new additions to the Websites as well as special offers and promotions of which you can take advantage. If at any time you decide you would rather not receive these types of communications from IPC or the FAF Group, you can revoke your election by clicking the unsubscribe link at the bottom of any IPC or FAF Group email, or by updating the contact preferences for your account (if you have one), or you may opt-out of mobile messages or alerts by following the instructions provided in the messages you receive. You may also opt out by contacting and providing your details to the Privacy Officer as set out below.

Contests and Surveys. From time to time, IPC may run voluntary contests or surveys through the Websites. Those contests or surveys may request Personal Information with your response, such as your name, address, home or mobile telephone number, and/or email address. IPC and the FAF Group will use the information provided solely in connection with the contest or survey conducted.

Cookies – Internet User. "Cookies" are pieces of information that a Websites sends to an individual's computer or other electronic device which allow the Websites to identify users and make their visits to the Websites more productive. IPC uses Cookies to help improve your future visits to the Websites.

The table below explains the cookies we use and why.

Cookie	Name	Purpose

Google Analytics	_ga _gid _utma _utmb _utmc _utmt _utmz	These cookies collect information in an anonymous form including the number of visitors to the site, how visitors reached the site and the pages visitors have visited.
Load Balancing	BIGipServer TS01	These cookies enable us to balance the workload by, for example, recording which server a user's browsing session has been allocated to ensure they only deal with a single server for the duration of their session.
Session ID	ASP.NET Session ASPXAUTH	These cookies are used by the ASP.NET framework to manage user session status while logged into the site, such as to help us recognize a visitor's language preference.
LiveChat	_lc.visitor_id.* Lc_sso* Lc_window_slate	These cookies are needed for the LiveChat feature on the website, allowing users to contact a live representative for support. Unique users are tracked, but the cookie does not contain personally identifying information about users.
Sitecore	sc_expview SC_ANALYTICS_GLOBAL_COOKIE	These cookies are used by Sitecore content management software to determine user experience settings and track user visits. Unique users are tracked, but the cookie does not contain personally identifying information about users.
MySubwayCareer.com Applicant site and Admin site	RequestVerificationToken ComeOrigin	These cookies are used to confirm that a visitor's request has already been validated and they have authorization to proceed and to track which region they are visiting from (either North American or International).

If you do not wish to receive a Cookie, or if you wish to set your browser to warn you each time a Cookie is being sent, or if you wish to disable all Cookies, you can adjust your internet browser settings to accomplish that. Please note that by disabling Cookies, you may not have access to some features available on the Websites.

Internet Protocol (IP) Address. Every computer and other electronic device which has a connection to the internet has an Internet Protocol (IP) address associated with it. IPC may use your IP address to help diagnose problems with IPC's server, to administer the Websites, and to maintain contact with you as you navigate through the Websites. Your device's IP address also may be used to provide you with information based upon your navigation through the Websites. IPC does not link IP addresses to any Personal Information, but does employ anti-fraud device fingerprinting technology which uses IP addresses to determine a device's geolocation.

D. Prospective and Actual Subway® Franchisees. IPC collects and uses Personal Information from prospective and actual Subway® Franchisees in order to provide services to them. IPC may collect this information from the Subway® Franchisees directly or IPC may receive it from the Co-op Group, the Subway® Group, the FAF Group, or other sources. IPC may use a prospective or actual Subway® Franchisee's Personal Information to respond to incoming service and support requests from such Franchisee, to communicate with such Franchisee regarding such Franchisee's account(s), to calculate, determine, and distribute such Franchisee's patronage dividend check, to collect Franchisee feedback, to conduct Franchisee satisfaction surveys, to offer promotions to such Franchisee, and to send other service informational mailings. IPC may also provide a Subway® Franchisee's Personal Information to a courier or freight forwarder in order to fulfil any order placed by such Franchisee.

E. Prospective Subway® Restaurant Employees. IPC collects and uses Personal Information from prospective Subway® Restaurant employees for the purpose of enabling them to be considered for employment at Subway® Restaurants of their choosing. This information includes name, address, home or mobile telephone number, email address, education jhistory, employment history, other employment-related information, and personal references. IPC shares this information with Subway® Franchisees selected by the user for the purpose of enabling the user to be considered for employment at Subway® Restaurants. IPC may also share this information with third party service providers, such as credit agencies, in order to perform background checks on the user in connection with his/her application for employment at Subway® Restaurants.

F. Customers of Subway® Restaurants. IPC collects and uses Personal Information from Subway® Restaurant customers in order to provide services to such customers. Personal Information collected from Subway® Restaurant customers includes Subway® Card and PIN numbers, and credit card information (for purchases of goods and services), products and services offered and purchased, enquiries and feedback.

G. **Sensitive Personal Information.** IPC does not intend to collect Sensitive Personal Information and will not otherwise share your Sensitive Personal Information with anyone unless you give your explicit consent to share your Sensitive Personal Information. The term "Sensitive Personal Information," includes, but is not limited to, information revealing racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, sexual orientation, disabilities, health and veteran status.

Storage, Disclosure, and Retention of Personal Information

A. Storage, Security, and Integrity of Personal Information. IPC and the Recipients may store or process your Personal Information in the U.S. and/or other countries. IPC uses commercially reasonable efforts to ensure that your Personal Information is safeguarded against loss, misuse, unauthorized access, disclosure, alteration, and destruction. IPC will endeavor to protect your Personal Information by using technical and organizational security measures appropriate to the sensitivity of the information in its control. These measures include safeguards to protect Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification, and destruction.

IPC safeguards your Personal Information on the internet by using industry-standard practices. While guaranteed security does not exist either on or off the internet, IPC takes commercially

reasonable steps to make the collection and security of such information consistent with this Privacy Policy and all applicable law.

The IPC-hosted Websites utilize a variety of different security measures designed to protect Personal Information by users both inside and outside of IPC, including the use of encryption mechanisms, such as Secure Socket Layers (SSL) and/or Transport Layer Security (TLS), password protection, and other security measures to help prevent unauthorized access to your Personal Information.

IPC also takes commercially reasonable steps to ensure that Personal Information is relevant for the purposes for which it is to be used and is accurate for its intended use.

B. Disclosure of Personal Information. IPC and the Recipients will not disclose your Personal Information to any third party except as described in this Privacy Policy, unless you request or otherwise consent to such disclosure, or unless IPC or a Recipient in good faith determines that such disclosure is required or authorized by law or necessary to: (a) comply with legal process served on IPC or the Recipients or other lawful requests by public authorities, including to meet national security or law enforcement requirements; (b) protect or defend the rights or property of IPC or the Recipients; or (c) act under expedient circumstances to protect the personal safety of IPC employees, Subway® Franchisees, Website users, and/or other members of the public.

C. Retention of Personal Information. IPC and the Recipients will retain your Personal Information only for as long as necessary to fulfil the purpose(s) for which it was collected and to comply with applicable laws and regulations. Your consent to IPC's and the Recipients' use of your Personal Information for such purposes(s) remains valid after termination of IPC's relationship with you.

IPC Websites and Third-Party Websites

For your convenience, IPC may include on the Websites links to other Websites. IPC provides these links as a convenience only and does not endorse the content or services offered by, or the privacy policies in place at, those other Websites. This Privacy Policy only applies to information gathered by or on behalf of IPC through the Websites or otherwise and does not apply to information gathered through linked Websites not operated by or on behalf of IPC, which have their own privacy policies. IPC has structured the Websites to make it reasonably clear when you leave the Websites and enter another Websites. IPC encourages you to review the privacy policy of each Websites you visit through a link from the Websites, to ensure you are comfortable with such policy, as it may differ substantially from this Privacy Policy. IPC is not responsible for the conduct or policy of any third party which operates a linked Websites.

Children and Data Collection

IPC will not knowingly allow anyone under thirteen (13) years of age to provide IPC with any Personal Information. Children under thirteen (13) years of age are required to obtain the express permission of a parent or guardian before submitting any Personal Information about themselves to the Websites. If a child under thirteen (13) years of age has provided IPC with Personal Information without the consent of a parent or guardian, the parent or guardian of that child should contact IPC's Privacy Officer as set forth below. IPC will use commercially reasonable efforts to promptly delete such child's Personal Information from its servers.

California Privacy Rights

California residents have the right under California Civil Code Section 1798.83 to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To request such details, contact VPS's Privacy Officer as set forth below. Please allow up to 45 days for a response.

Nevada Residents

Nevada residents have the right under Nevada law to direct us not to make any "sale" of any "covered information" that we have collected, or that we may collect in the future, from or about you. The term "sale" is limited to our exchanging your information for money to anyone who intends to license or sell that information to other people. It does not include our disclosing your information to anyone who works with us to process your information, or to any of our affiliates. "Covered information" may include personally identifiable information in the form of your first and last name, home or other physical address, email address or telephone number, and any other information that we have collected or may collect from you in combination with any of the other identifiers listed above that are unique to you and would identify you.

To exercise this right, contact IPC's Privacy Officer as set forth below. We may ask you to follow up telephone requests with an email confirmation. We may also ask you to provide us with information that will help us identify you in order to verify your request. *We will never ask you for a copy of your photo identification, your Social Security Number, or your full account number with us.*

Please allow up to 45 days for a response to your verified request.

Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA")

Canada has enacted federal privacy legislation, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), which incorporates ten (10) "Fair Information Principles" regarding your Personal Information. IPC adheres to these Fair Information Principles for Personal Information collected and/or transferred from Canada, which are as follows:

Principle 1 - Accountability. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the fair information principles.

Principle 2 - Identifying Purposes. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 - Consent. The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Principle 4 - Limiting Collection. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 - Limiting Use, Disclosure and Retention. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6 - Accuracy. Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 - Security Safeguards. Personal information shall be protected by security safeguards appropriate to the sensitivity of the Personal Information.

Principle 8 - Openness Concerning Policies and Practices. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 - Individual Access to Personal Information. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance. An individual shall be able to address a challenge concerning compliance with the fair information principles to the designated individual or individuals accountable for the organization's compliance.

Privacy Shield

IPC complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. We are committed to subjecting all personally identifiable information received from European Union member countries, and Switzerland, to the applicable Privacy Shield Principles.

To learn more about the Privacy Shield program and to view our certification, visit https://www.privacyshield.gov/list.

IPC is responsible under the Privacy Shield Frameworks for the processing of personally identifiable information it receives and subsequently transfers to a third party acting as an agent on its behalf. We comply with the Privacy Shield Principles for all onward transfers of personally identifiable information received from the E.U. and Switzerland, including the onward transfer liability provisions. We are also subject to the investigatory and regulatory enforcement powers of the U.S. Federal Trade Commission with respect to personally identifiable information received or transferred pursuant to the Privacy Shield Frameworks. In certain situations, we may be required to disclose such information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If there is any conflict between the terms of this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern with respect to personally identifiable information received from the E.U. and Switzerland.

To learn more about how to file a complaint under the Privacy Shield Framework and other potential recourse mechanisms, see the section titled "Questions & Complaints" below.

Questions / Complaints

If you have any questions about IPC's privacy practices, or you wish to access, correct, or delete your Personal Information, please contact the IPC Privacy Officer as set forth below.

Likewise, any complaints about IPC's privacy practices should also be directed to the IPC Privacy Officer. The IPC Privacy Officer will endeavor to respond to all questions, comments, and concerns as soon as reasonably practicable. The Privacy Officer will also endeavor to investigate and attempt to resolve any complaints within 45 days.

If you are an E.U. resident, you have the right under the GDPR to lodge a complaint with your local supervisory authority for data protection.

If your information is subject to the E.U.-U.S. or Swiss-U.S. Privacy Shield Frameworks described above, you may lodge a complaint with the U.S. Federal Trade Commission. Under certain conditions, and when all other dispute resolution procedures have been exhausted, you may also be entitled to invoke binding arbitration, at no cost to you, through the International Center for Dispute Resolution - American Arbitration Association. For more information, visit:

https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint,

https://ftccomplaintassistant.gov/#crnt&panel1-1, and

https://go.adr.org/privacyshieldfiling.html.

Contact Information

The IPC Privacy Officer can be reached by mail, telephone, facsimile, or email, as follows:

IPC Privacy Officer

Independent Purchasing Cooperative, Inc.
9200 South Dadeland Boulevard, Suite 800
Miami, FL 33156
Telephone: (888) 445-9239
Facsimile: (305) 670-4465
Email: privacyofficer@ipcoop.com

Changes to This Privacy Policy

IPC will update this Privacy Policy occasionally. When IPC posts changes to this Privacy Policy, It will also update the "Revised" date below. If IPC makes material changes to this Privacy Policy, IPC will notify you by email or by means of a notice on the Websites describing the material changes. IPC encourages you to review this Privacy Policy periodically to be informed of how IPC is protecting your information and to be aware of any changes to the Privacy Policy. Any changes to this Privacy Policy are effective immediately upon being posted to the Websites. Your continued use of the Websites after the posting of any revised Privacy Policy shall constitute your agreement to be bound by any such changes.

Revised April __, 2020