WORKFORCE PRIVACY NOTICE

V3.0
Effective Date: January 1, 2023

Your privacy is important to us, and we're committed to the protection of your privacy in relationship to your employment application, employment, and post-employment at Staples. This Privacy Notice describes how our “Company” (which includes Staples, Inc., and US Retail as well as applicable subsidiaries, affiliates, and related entities) processes Personal Information about you as an applicant, a current or former employee, or other members of our workforce ("Workforce"). The Company recognizes its Workforce, representatives, agents, and service providers also have a responsibility in protecting Personal Information.

The Company and the Workforce will respect the confidentiality of the Personal Information placed in its care. The rights and obligations described in this Privacy Notice will apply to all Workforce members. The Company and the Workforce must comply with this Privacy Notice.

“Personal Information” refers to any information pertaining to an individual, including identifiers, commercial information, biometric information, internet/network activity, geolocation data, audio/visual data, professional/employment information, education information, inferences, and sensitive personal information.

This Privacy Notice describes how we collect, use, disclose, and protect your Personal Information, and the choices you have regarding your Personal Information.

1. Personal Information Collected and How It Is Collected

Types of Personal Information that we, or our Service Providers on our behalf, may collect:

- Name and contact information such as postal address, email address, and phone number
- Identifying information such as social security number and driver’s license number
- Employment authorization and IRS Form I-9 information such as birth certificate and passport
- Non-work-related contact information such as personal email address and personal phone number
- Employment history such as previous work experience
- Education history such as schools attended, transcripts, and degrees or certifications obtained
- Work-related expenses such as travel records and expense reports
- Compensation information such as salary, 401K, benefits, hours worked, direct deposit information
- Benefits information such as programs enrolled in, beneficiaries, and emergency contacts
- Protected information such as race, ethnicity, gender, religion, disability status, veteran status, and date of birth/age or other sensitive or protected category information that you might voluntarily disclose
- Inferences such as results from personality assessments and leadership assessments

- Digital activity such as system logs of activity, URLs visited, IP address, and remote access
- Preferences such as hobbies, leisure activities, organization membership, and dietary choices
- Professional employment data such as union membership, job performance records, and promotions
- Recordings from video conferences, CCTV cameras, and voice recordings

Personal Information is collected from the following:

- **Information You Provide Us Directly.** We collect Personal Information which you provide us directly, for example, in connection with employment application or onboarding, benefits and perks, travel profiles, work products, security/safety procedures, surveys, contests, event registration, or application for a membership program.

- **Information Collected Through Automated Technologies.** For example, we use Mobile Device Management and Audit/Monitoring/Logging tools to manage access to company information/networks/systems. We collect logs of application/network/internet activity and physical security access as well call recordings. We may also collect information pertaining to CCTV and facial recognition, fleet driver monitoring including exterior/interior video footage, and employment application videos.

- **Information We Receive from Other Parties.** For example, at times Staples may also receive personal information from its affiliates, publicly available sources, or third parties for purposes such as background checks, application references, career assessments, and benefits administration.

Minors:
Our business practices, websites and online mobile applications are not directed toward children under 13 years of age. We do not knowingly collect Personal Information of children under 13 years of age without parental/guardian consent.

2. How We Use Personal Information

Personal Information may be collected, used, and disclosed for purposes pertaining to the Individual's employment relationship with the Company, including but not limited to:

- Determining eligibility for initial employment, including the verification of references and assessing qualifications
- Administering the employee hiring/onboarding process
- Conducting performance management/appraisals and determining performance requirements
- Administering and processing employee payroll, benefits, and compensation analysis
- Processing employment related claims (e.g., worker compensation, insurance, etc.)
- Protecting the safety and well-being of our Workforce
- Establishing and tracking training/development requirements
- Gathering evidence for disciplinary action/termination or to appeal a disciplinary action, legal requirements, investigating/resolving issues

- Conducting crisis management including communicating with emergency contacts and workforce members in emergency situations
- Compiling company directories
- Communicating or sending Staples-related mailings or shipments to Workforce home addresses
- Protecting the security of company-held information and preventing fraud
- Providing a safe and secure work environment
- Complying with applicable labor or employment requirements
- Addressing inclusion and diversity company objectives and values
- Complying with appropriate legal, regulatory, and fiscal obligations including responding to audits, requests, and investigations
- Auditing, monitoring, and logging device, system, and network usage
- For other legitimate purposes reasonably required for day-to-day operations, such as accounting, financial reporting, process improvement, and business planning

3. When We Disclose Personal Information

We may disclose your Personal Information to other parties for certain purposes, including:

- Within our family of companies to support entity level business processes and reporting
- To process transactions or provide products/services on the behalf of the Company
- To our affiliates, employees, contractors, consultants, and other parties who require certain information to assist with managing the Workforce and/or your relationship with us
- Where the disclosure is for the purpose of employment verification/references to agencies and prospective employers
- Where the disclosure is directed to administer health and other benefits
- To support diversity and inclusion functions and reporting
- In an emergency to your emergency contact or where necessary to protect the physical safety of any person or group of persons
- For purposes of complying with applicable public health regulations or requirements.
- To notify you of products or services that may be of interest to you
- To solicit feedback from you and perform demographic analysis on feedback responses
- In connection with a merger, acquisition, transfer of assets, or sale involving all or a portion of the Company
- To our current or prospective business partners and customers where relevant to your role
- To detect, prevent, or mitigate potential fraud, security, ethics, or technical issues/violations
- To assist with the improvement of business processes
- Where the disclosure is in accord with the purposes for which the Personal Information was originally collected
- Where the Company is permitted or required to do so by applicable legislation or regulation
- Where the disclosure is required by authorized government representatives who are acting to enforce any federal or state law

- Where the Company is required to comply with valid court orders, warrants, or subpoenas or other valid legal processes
- Where the Individual who is the subject of the disclosure has provided consent

4. Your Choices Regarding Your Personal Information

a. To Stop Certain Collection and Use of Your Personal Information:

- You can stop promotional emails from us by using the “unsubscribe” link in the footer of those promotional emails or contacting us if you have questions.
- You can stop text messages by replying “STOP” to our text messages
- You can request to stop postal mail by contacting to us as noted in section 8
- You can stop in-app push notification from workforce mobile apps by adjusting your Notification Settings

b. To Correct Your Personal Information

You can request that inaccuracies pertaining to your Personal Information be corrected.

You can update some information by logging into your Associate Connection account. You can also contact HRServices@Staples.com for additional guidance.

To prevent unauthorized changes, we may ask for certain information to verify your identity before we process such requests.

We may not fulfill your request in some cases, for example, if it requires a disproportionate technical or practical cost or effort or if it conflicts with our legal obligations or business requirements.

c. Optional Personal Information

Where the collection of Personal Information is required to comply with legal or contractual obligations, or to manage the employment relationship, the provision of Personal Information generally is mandatory. In some other cases, provision of requested Personal Information is optional; however, failure to provide the information may result in your inability to fully participate in the activity or benefit for which the Personal Information is requested, such as an optional benefit program.

5. How We Protect Your Personal Information

The Company takes the security, privacy, and protection of Personal Information seriously. We employ physical, organizational, technological, and administrative safeguards to help protect your Personal Information.

Some of these protocols may include, but not be limited to the following:

- Physical security including badge access to facilities and sensitive areas, locked storage areas, and security guard presence
- Organizational security including security clearances and role-based access controls
- Technological security including passwords, network monitoring/logging, and data encryption

- Administrative security including the enforcement of various policies and procedures

While we strive to protect your Personal Information, we cannot guarantee or warrant the security of your Personal Information.

Please use caution when sharing your information with others and take appropriate measures to protect your own Personal Information. For example, keep your passwords secure and confidential and don't divulge them to anyone.

If you think the Personal Information you provided to us has been improperly accessed or used, please contact HRServices@Staples.com immediately.

If you believe the company's systems or information may be at risk or if additional guidance is needed, please contact HR Services (HRServices@Staples.com) or the Privacy Team (Privacy@Staples.com) immediately.

6. Workforce-Specific Disclosures

a. California Residents

California Consumer Privacy Act of 2018 (CCPA)/California Privacy Rights Act of 2020 (CPRA)

This section applies to residents of California, in addition to all other non-state specific information contained in this Notice.

The following section describes:

1. Categories of Personal Information We Collect
2. Examples of Specific Personal Information that may be Collected
3. Categories of Sources from which Personal Information is Collected
4. Purpose of Collecting the Personal Information
5. Categories of Other Parties to whom Personal Information may be Disclosed

Not all categories or examples of specific Personal Information may be collected about you depending on how you interact with us.

Categories of Personal Information We Collect	Examples of Specific Personal Information that may be Collected	Categories of Sources from which Personal Information is Collected	Purpose of Collecting the Personal Information	Categories of Other Parties to whom Personal Information may be Disclosed
Identifiers	Full Name, SSN, Driver's License Number, Banking Information, Birth Date, Passport, Birth Certification, Personal Contact Information Such as Address, Email Address, Telephone Numbers, Employee ID, Staples Contact Information	From You and Service Providers (e.g., benefits providers, recruiting agencies, etc.)	To Uniquely Identify an Individual in Support of Business Activities and for Employment Authorization	Benefits Providers Recruiting Agencies Survey Management Vendors Government Agencies for employment purposes

Commercial Information	Perks Activity, Company Purchases in your Employment Role, Travel Records, Sweepstakes/Survey/ Contest Submissions	From You (when you participate in any of our programs)	To Understand Participation in Company Programs and In Support of Business Activities	Program Service Providers Travel Vendor
Biometrics	Facial Template used for Facial Recognition in some Facilities	From our service providers (e.g., facility security vendor)	For Security, Access Control, and in Support of Business Compliance/Activities	Facility Security Service Providers
Characteristics of Protected Classifications	Demographic information such as age ranges, marital status, etc.	From You and Service Providers (e.g., wellness program or benefit providers)		Benefits Providers Wellness Program Providers Survey Management Vendors
Internet or Other Electronic Network Activity	IP Address, Internet/ System/Application Activity Logs, Badge Logs, Browsing History	From You, Your Devices (when you access our network) and Service Providers (e.g., network security vendors)	For Security and Fraud Detection and In Support of Business Compliance/Activities	Network Service Providers Security Service Providers
Geolocation Data	Device Longitude and Latitude, IP Address Correlations	From You, Your Devices (when you access our websites or mobile apps), Service Providers (e.g., data analytics providers, fraud prevention companies)	For Security and Fraud Detection and In Support of Business Compliance/Activities	Network Service Providers Security Service Providers Fraud Prevention Service Providers
Recordings/ Electronic Communications (e.g. audio, visual, chat, etc.)	Voice or Chat Recordings, CCTV Recordings, Dash Cam Interior/Exterior Video, Photographs	From You (when you call the Help Center or when you visit some of our facilities), Service Providers (e.g., driver safety vendor, call recording software providers, etc.)	For Security, Quality Assurance, Training, and in Support of Business Compliance/Activities	Call Recording Service Providers Driver Safety Program Service Providers Facility Security Service Providers
Professional or Employment-Related Information	Employment History, Job Title, Performance Reviews, Resume, Career Assessments, Background Checks, Work Eligibility Evidence, Work Permit Application/Status	From You (e.g., when you apply for a job), Service Providers (e.g., recruiting agencies)	For Employment Evaluation, Onboarding, Talent Management and In Support of Business Compliance/Activities	Recruiting Agencies Talent Management Service Providers Government Agencies for employment purposes
Education Information	Education Transcripts, Certifications	From You (e.g., when you apply for a job), Service Providers (e.g., recruiting agencies)	For Employment Evaluation, Onboarding, Talent Management, and In Support of Business Activities	Recruiting Agencies Talent Management Service Providers
Inferences	Leadership Qualities, Interests	Internal Teams and Service Providers (e.g., consulting services)	For Succession Planning, Talent Management and In Support of Business Activities	Talent Management Service Providers
Sensitive Personal Information*	Race, Ethnicity, Precise Geolocation	From You and Your Devices (e.g., when submitting your time reporting remotely)	To Support Inclusion and Diversity Programs, to Support Payment Processing, Delivery Driver Safety Monitoring, etc.	Survey Management Vendors Consulting Services Vendors Time Tracking Vendors

The above categories are intended to encompass the Personal Information described in subdivision (e) of Section 1798.80 of the California Civil Code.

*We do not collect or process Sensitive Personal Information for the purpose of inferring characteristics about you.

California residents have the following rights under the CCPA/CPRA:

- **Right to Know and Access.** You have the right to confirm whether or not we are processing your personal information and to know what personal information the business has collected about you. While our table below describes the personal information we collect about you, you have the right to make a request to know and get access to information that is specific to you, should we have any.
- **Right to Delete.** You have the right to request that we delete personal information we have collected from you or obtained about you, subject to certain exceptions. For example, we will not delete any personal information required to provide our existing services to you or that we must maintain to comply with our legal/financial obligations.
- **Right to Correct.** You may request that we correct inaccurate information we maintain about you, subject to some exceptions and, if necessary, independent verification.
- **Right to Opt-Out of the Sale/Sharing.** If we have sold or shared personal information about you, you have the right to opt out of the sale or sharing of that personal information.
- **Right to Non-Discrimination.** You have the right not to be discriminated against if you exercise any of these rights. Please note that a legitimate denial of a request to know or access, delete, correct, or opt out is not discriminatory, nor is charging a fee for excessive or repetitive consumer requests as permitted by the CCPA/CPRA.

California residents may submit your request to Know/Access, Delete, Correct, Opt-Out of the Sale/Sharing of your Personal Information by:

1. Submitting an online request here: California Workforce Privacy Rights Request
2. Submitting a phone request by calling 1-888-490-4747

We will take reasonable steps to verify your above request prior to fulfilling it by requiring a response to a confirmation email sent to the email address on the request. For purposes of verifying your identity, we will request that you provide personal information we already have on file including, but not limited to, your name, email address, and phone number. We may also request other verification information, such as your employee ID and term of employment. We will respond to your request and let you know if we need additional information.

Authorized Agent:
You may designate an authorized agent to exercise your rights under the CCPA/CPRA on your behalf. You must provide the authorized agent written permission to exercise your rights under the CCPA/CPRA on your behalf and we may deny a request from an agent on your behalf if we cannot verify that they have been authorized by you to act on your behalf. Even if you use an authorized agent to exercise your rights under the CCPA/CPRA on your behalf, pursuant to the CCPA/CPRA we may still require that you verify your own identity directly to us. This provision does not apply if you have provided a power of attorney under the California Probate Code.

Minors:
We do not knowingly share or sell the Personal Information of children under 16 years of age.

Notice of Financial Incentive:
We may provide price discounts, coupons, services, and other perks to our workforce and for members of our wellness programs. Through these offerings, you may provide us with Personal Information depending on how you choose to interact with us when and after you opt-in to our programs. There is no obligation to opt-in, and you may opt-out at any time. The details of the programs are contained in the program offerings. We offer these programs, among other things, to enhance our relationship with you so you can enjoy more of our products/services at a lower price. The value to our business of any individual consumer's data is dependent on several factors, including, for example, whether and to what extent you take advantage or opt out of any offerings and whether we are able to enhance the data through our efforts described in this Privacy Notice. While we do not calculate the value of consumer data in our accounting statements, we provide this good faith summary for California residents. To the extent we create overall business value from our programs that could be directly or reasonably related to the value of consumer data, the method for calculating the value would include: a) costs related to maintaining the program including but not limited to IT infrastructure, delivery of offers, and marketing activities to enhance consumer data; b) whether the sales generated by the program exceeds the cost to us of offering the program including value of discounts to consumer; and c) value of the insights we are able to create based upon aggregate data.

Data Retention:
We retain all categories of your personal information for as long as is necessary, even if you are no longer an active workforce member, to provide the goods and services and to fulfill the transactions you have requested of us, and to support other necessary purposes such as:

- providing related business processes (such as returns or exchanges),
- resolving disputes and enforcing our agreements,
- fulfilling our legitimate interests (such as improving our products and services)
- responding to any questions, complaints or claims made by you or on your behalf,
- preventing fraud, and
- complying with our legal obligations.

In determining how long to retain information, we may consider various criteria such as the amount, nature and sensitivity of the information, and the potential risk of harm from unauthorized use or disclosure of the information.

The purposes and criteria for which we process the data may dictate different retention periods for the same types of information. For example, we retain your email address as an authentication credential (where applicable) as long as you have an account with us and an additional period of time after that for our legitimate interests and for our fraud and legal compliance purposes. We may also retain cached or archived copies of your information.

Non-Discrimination:
We will not discriminate against you for exercising any of your CCPA/CPRA Rights and we will not deny you goods or services, charge you a different price, or provide you with a lesser quality of goods or services if you exercise any of your CCPA/CPRA Rights.

b. United Kingdom (UK) and European Union (EU) Residents

In Europe and the UK, we process sensitive data on the following legal grounds, consistent with local data protection law: (i) explicit consent; (ii) to carry out our obligations and exercise specific rights in the field of employment and social security and social protection law and/or a qualifying collective agreement; (iii) to protect the vital interests of the you or of others where you are physically or legally incapable of giving consent; (iv) where applicable, you have made the data public; (v) to establish, exercise, or defend a legal claim or whenever courts are acting in their judicial capacity; (vi) for substantial public interest as permitted by local data protection law; and (vii) for assessment of the working capacity of the employee.

EU residents have the right to lodge a complaint with an EEA supervisory authority (https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm) and UK residents may lodge a complaint with the Information Commissioner's Office (https://ico.org.uk/make-a-complaint/). We would, however, appreciate the opportunity to first address your concerns and would welcome you directing an inquiry first to us at Privacy@Staples.com.

c. Other Residents

Where the Company has Workforce living and working in different jurisdictions the specific rights and obligations of Workforce may vary between jurisdictions.

The Company may be subject to the privacy legislation in jurisdictions in which the Company operates.

7. How to Contact Us

This Privacy Notice applies to Staples, Inc., and its affiliated companies.

Please direct any questions, complaints, or concerns regarding this Privacy Notice to any of the following:

Primary Contact by Email:	Privacy@Staples.com
Secondary Contact by Email:	HRServices@Staples.com
Alternate Contact by Phone:	1-888-490-4747
Or by Writing to:	Staples Inc. Privacy and Compliance 500 Staples Drive Framingham, MA 01702

If you have any questions pertaining to the collection, sharing or protection of your Personal Information, please contact Privacy@Staples.com.

Upon receiving a request, we may contact you directly to follow up on your request. We reserve the right to take reasonable steps to verify your identity prior to granting access or processing changes or corrections.

8. Workforce Privacy Notice Updates

This Privacy Notice may change from time to time, including for the purpose of reflecting changes in our legal or regulatory obligations, and we will post the updated Notice on applicable web properties and make it otherwise available as appropriate. Recent changes to the Privacy Notice will be documented below. Each version of this Privacy Notice will be identified by its effective date displayed at the top of this Privacy Notice.

What has changed:

V3.0	January 2023	Updates for CCPA/CPRA
v2.0	September 2022	General Updates
v1.0	January 2020	Workforce Privacy Notice