Workforce Privacy Policy and Notice at Collection

Effective Date: 11/05/2024

This Workforce Privacy Policy and Notice at Collection ("**Policy**") describes how WP Company LLC ("**The Washington Post**", "**Company**", "**we**", "**us**" and "**our**") collects, uses, and discloses information about our current and former employees, applicants for employment at The Washington Post, contractors, consultants, interns, and other workforce members (and their beneficiaries and emergency contacts) in the context of our working relationship with the relevant individuals.

We may update this Policy at any time. We may also provide you additional privacy notices regarding our collection, use or disclosure of information. If you are located outside the United States, you may be subject to an additional privacy notice (such as in connection with your employment contract). To the extent such additional privacy notice conflicts with this one, that notice will govern as to the conflicting provision. Please contact us using the contact information below with any questions regarding this Policy.

Please read this Policy and any other privacy notices carefully. This Policy does not form part of any employment contract or contract to provide services. This Policy does not apply to our handling of data gathered about you in your role as a user of our consumer-facing services. When you interact with us as in that role, The Washington Post Privacy Policy applies.

Depending on where you live, you may have certain rights with respect to your information. Please see Section 5 below for more information about your rights. If any provision below conflicts with a legal requirement, then the Company will comply with the applicable law.

1. Types of Personal Information We Handle

We collect, store, and use various types of information that identifies, relates to, or could reasonably be linked to you ("**personal information**") in connection with your application or employment with us. We collect such information either directly from you or (where applicable) from another person or entity, such as professional networking websites, job posting websites, employment agencies, recruitment companies, or others who provide references. The types of information we have or will have about you depends on your role with us and country of your employment. We will collect additional personal information throughout the course of your application, employment, or other provision of services to us.

The information we collect from and about you includes, where applicable:

- **Identifiers** such as real name or alias, business or personal address, telephone numbers, and email addresses (and such information about your emergency contacts), employer identification number, driver's license number, passport number, Social Security number, birth certificate number, and/or other form of government-issued identification.

- **Professional or employment-related information**, including:
    - **Recruitment, employment, or engagement information** such as application forms and information included in a resume, cover letter, or otherwise provided

through the application and recruitment process, information about your eligibility to work in the United States, such as information related to citizenship and/or immigration status, references, our evaluations of your performance during the interview process, and background screening results (including any criminal convictions).

- **Career information** such as job titles, work history, salary history, work dates and work locations, employment, service, or engagement agreements, appraisal and performance information, information about skills, qualifications, experience, publications, speaking engagements, and preferences (e.g., mobility), life insurance policy number, absence and leave records, disciplinary and grievance information, and termination information.
- **Financial information** such as salary, payroll, pension or retirement contribution information, tax information, expense information, and financial institution account number.
- **Union membership** such as role eligibility and dues paying elections.

- **Education information** such as institutions attended, degrees, academic record, certifications, licenses, transcript information, and professional memberships.
- **Business travel and expense information** such as travel itinerary information, corporate expenses, and Company credit card usage.
- **Audio or visual information** such as CCTV footage, as well as other information relating to the security of our premises, video or audio recordings, recorded presentations in which you participate, and photographs taken at Company functions or for Company identification or other materials.
- **Internet and electronic network, and device activity and device information and related identifiers**, such as information about your use of the Company network, information, and communication systems, including user IDs, passwords, IP addresses, device IDs, web logs, metadata, and audit trails of system access.
- **Geolocation information** such as general geolocation information.
- **Legally protected classification information** to the extent required or as permitted by law and voluntarily provided such as, gender identity/expression, sexual orientation, marital status, military service, nationality, ethnicity, veteran status, request for family care leave, criminal history, and other information to help us monitor compliance with equal opportunity legislation.
- **Health information** about you, and, if applicable, your beneficiaries, such as medical conditions and other information provided in statement of health forms, disability status, vaccination status, health and safety incidents, or accidents, sickness records, and health issues requiring adaptations to your working environment or working practices.
- **Other information that directly or indirectly identifies you**, such as date and place of birth, citizenship, and permanent residence (and such information about your

dependents or emergency contacts); and information on any publicly available social media profile of yours that mentions your connection to us.

2. How We Use Personal Information

We have or will collect, use, share, and store personal information for our legitimate business purposes, which include, where applicable:

- **Engaging in the recruitment process,** including communicating with you, interviewing, and selecting and hiring new personnel.

- **HR management and administration,** including training, compensation and benefits, leave, scheduling, career development, performance appraisals and recognition, investigating and resolving inquiries and complaints, providing references, succession planning, organizational changes, recruiting activities, assessing hiring needs, preparing analyses and reports, and communicating with our workforce (whether by email or other means) about updates or relevant information about perks, benefits and discounts, and changes to Company products and services.

- **Business operations**, including providing and monitoring IT systems for any lawful purpose, maintaining accounts and internal directories, crisis management, protecting occupational health and safety, participating in due diligence activities related to the business, business succession planning, and conducting internal analyses and audits.

- **Security operations,** including detecting security incidents, debugging and repairing errors, and preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution; monitoring and controlling access to company premises and locations (including through use of CCTV); and safeguarding the Company and its locations, services, personnel, and others.

- **Legal compliance and assistance,** such as complying with anti-bribery, tax, social security and immigration obligations, responding to and cooperating with legal or regulatory requests and investigations, and seeking legal advice and representation.

- **Exercising or defending our legal rights,** including seeking legal advice from our external lawyers or in connection with litigation with you or a third party.

We may also use personal information for any other legally permitted purpose if we have your consent.

Certain information we collect may be considered "**sensitive personal information**" under California law. We collect and process such information only for our legitimate business purposes and do not process such information for purposes for which the "right to limit" applies under California law. We use the following information that may be considered "sensitive" as legally necessary, in the following ways:

- Social Security number or passport information for legal compliance, payroll, benefits, tax, and immigration purposes.

- Union membership information for legal compliance and compliance with collective bargaining agreements or to exercise rights thereunder.

- Health information, which may include disability status, to provide reasonable workplace accommodations and manage absences, for workplace health and safety purposes, and for compliance with applicable law and contracts or to exercise rights thereunder.
- Racial/ethnic origin, sexual orientation, disability, and military or veteran status for equal opportunity and diversity and inclusion purposes and compliance with applicable law or to exercise rights thereunder.

Biometric Authentication Technologies. You may have the option to use biometric authentication on Washington Post-issued devices or your personal devices that you use for work, such as TouchID or FaceID on certain Apple devices and Windows Hello on certain Windows devices. These technologies may collect data, such as fingerprint or face scans, that may be considered "biometric data," "biometric information," or "biometric identifiers" under certain laws (collectively, "Biometric Data"), and they process such data for security and authentication purposes. If you choose to use these technologies, your Biometric Data is processed locally on your device and stored on your device in an encrypted form. **The Washington Post does not collect any such Biometric Data and cannot and will not access any such Biometric Data**, even if the Washington Post provides or possesses the device on which the Biometric Data is stored. For more information about biometric authentication technologies and the security measures they employ, please consult documentation made available by the relevant technology or device manufacturer (which may be available on the manufacturer's website).

3. How We Disclose Personal Information

We may disclose certain personal information to the following types of entities or in the following circumstances (where applicable):

- **Internally**: to people within certain parts of the company to carry out the purposes described in this Policy, including to your manager, human resources, as well as personnel within the Company, such as payroll, IT, legal and finance.

- **Vendors**: such as background check companies, security providers, information technology providers, travel management companies, employment businesses (e.g., recruiting contractors or agency workers) that provide us with services relevant to recruiting and hiring, compensation and benefits providers, corporate card issuers, human resource suppliers, group benefit plan carriers, employment businesses (for contractors or agency workers), content providers, information technology providers such as data storage and hosting providers, and security providers.

- **Recruiters**: to the extent you are working with a recruiter in connection with your application for employment and your recruiter is authorized by you to obtain feedback from us regarding your application and interview process.

- **Legal compliance and exercising legal rights**: (i) when required to do so by law, regulation, or court order; (ii) in response to a request for assistance by the police or other law enforcement agency; (iii) to seek legal advice from our external lawyers or in connection with litigation with you or a third party; or (iv) as otherwise necessary to exercising our legal rights or to protect the Company or its employees.

- **Business operations** to provide another entity (such as a potential or existing business counterparty or customer) with a means of contacting you in the normal course of business, for example, by providing your contact details, such as your phone number and email address.

- **Business transaction purposes**: in connection with the sale, purchase, or merger of all or a portion of our Company.

- **Consent**: with your consent and as permitted by law, we may disclose personal information to any other parties in any other circumstances.

4. Data Retention

The personal information we do or will collect, including sensitive personal information, will be retained for as long we determine is necessary to satisfy the purposes for which it was collected and for our legal obligations. As described above, these purposes include our business operations and complying with reporting, legal and accounting obligations. In determining how long to retain information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the personal information, the purposes for which we process the personal information and whether we can achieve those purposes in other ways, the applicable legal requirements, and our legitimate interests.

5. Your Privacy Rights

Certain jurisdictions, such as California, the European Union, and the United Kingdom, may provide you with privacy rights under applicable data protection or privacy laws regarding your personal information. In particular, if you are from a certain jurisdiction, you may have the right to request some or all of the following:

- Information about the processing of your personal information;

- Access to your personal information;

- To correct personal information that is inaccurate;

- To have your personal information deleted;

- To object to the processing of your data; and

- To object to how your personal information is used in automated decision making, if applicable.

These rights may be limited, for example, if fulfilling your request would reveal personal information about another individual, or if you ask us to delete personal information we are required by law to retain or which we need to defend claims against us.

Exercising Your Rights. To exercise any of these rights, please contact us by using the contact details below. We will respond to requests in accordance with the requirements of applicable data protection and privacy laws.

Verification. We will respond to your request in compliance with the requirements of applicable law. Please note that to fulfill your request, we may need you to provide certain personal information to verify your identity. We or our partners will verify your identity by asking you to authenticate your identity via standard authentication procedures. For example, we may ask for your email address or certain evidence of identification. We also may use a third-party verification provider to verify your identity.

Authorized Agent. Depending upon applicable data protection and privacy law, you may permit an authorized agent to submit a request to know or to delete your personal information. If we receive a request on your behalf, we may ask that person to give us proof that you gave that person written permission to make a request for you. If that person does not provide us with written proof, we may deny their request so that we can protect your personal information.

Non-Discrimination. If you make a request under applicable law, you have the right not to be discriminated against (as set forth in applicable law).

Automated Decision-Making. We generally do not engage in automated decision-making, as that term is defined by applicable state privacy laws. If we make use of automated decision-making, you will be informed through a separate privacy notice.

Questions or Concerns. If you have any concerns or complaints about our data processing activities, we urge you to first try to resolve such issues directly with us by contacting us as set forth in Section 7 below at any time. However, if applicable, you may make a complaint to the data protection supervisory authority in the state or country where you are based.

6. No Sale or "Sharing" of Personal Information

California law also places certain obligations on businesses that "sell" personal information to third parties or "share" personal information with third parties for cross-context behavioral advertising as those terms are defined under the CCPA. We do not "sell" or "share" the personal information covered by this Policy and have not done so in the twelve months prior to the effective date of this Policy.

7. How to Contact Us About This Policy

If you have questions about our collection, use, or disclosure of personal information, or to exercise one of the rights above, please contact us in one of the following ways:

- By phone: 1-855-699-5033
- By email: HR@washpost.com