

California Job Applicant Privacy Policy and Notice

Crestron Electronics, Inc.

Last updated: 12 January 2023

Crestron Electronics, Inc. (the “**Company**” or “**we**”) provide this California Job Applicant Privacy Policy and Notice (“**Notice**”) to describe our privacy practices with respect to our collection of Personal Information as required under the California Consumer Privacy Act as amended by the California Privacy Rights Act (“**CCPA**”). This Notice applies only to job applicants and candidates for employment who are residents of the State of California (“**Consumers**”) and from whom we collect “**Personal Information**” as defined in the CCPA. We provide you this Notice because under the CCPA, California residents who are job applicants qualify as Consumers. For purposes of this Notice, when we refer to Consumers, we mean you only to the extent you are a job applicant who resides in California.

1. Collection of Personal Information

1.1 We may collect Personal Information from or about you in connection with your job application from a variety of sources, including, but not limited to, on our on-line application, other materials you provide or submit as part of your application, your communications with us via mail, email, or telephone, and through third party vendors we utilize as part of the job application process. The Company may collect, receive, maintain, and use the following categories of Personal Information for any of the purposes listed in **Section 4** below and to the extent permitted under applicable law. In the last 12 months we may have collected the categories of personal information below from or about job applicants and may have disclosed such information to the categories of third parties identified in **Section 3**.

Category	Examples
Personal Identifiers	Name, alias, social security number, date of birth, driver’s license or state identification card number, passport number.
Contact Information	Home, postal or mailing address, email address, home phone number, cell phone number.
Pre-Hire Information	Information provided in your job application or resume, employment and education history, information gathered as part of background screening and reference checks, information contained in candidate evaluation records and assessments, information in work product samples you provided, voluntary disclosures by you.
Inferences	Based on analysis of the personal information collected (but not based on sensitive personal information), we may develop inferences regarding job applicants’ predispositions, behavior, attitudes, intelligence, abilities, and aptitudes for purposes of recruiting and hiring assessments and decisions.

1.2 The above categories of Personal Information may include the following Sensitive Personal Information:

Social security, driver’s license, state identification card, or passport number.



1.3 Personal Information *does not* include:

- (a) Publicly available information from government records.
- (b) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the job applicant or from widely distributed media.
- (c) Information made available by a person to whom the job applicant has disclosed the information if the job applicant has not restricted the information to a specific audience.
- (d) De-identified or aggregated information.

2. We May Collect Your Personal Information from the Following Sources:

- (a) You, the job applicant, voluntarily submitting information for job application purposes.
- (b) Background check, credit and consumer reporting agencies.
- (c) Recruiters or staffing agencies.
- (d) Personal references and former employers.
- (e) Other third party vendors we utilize as part of the job application process.

3. We May Disclose Your Personal Information to the Following Categories of Third Parties, Service Providers, and Vendors:

- A. Professional service providers including attorneys, accountants, auditors, insurance agents or carriers, administrators, and brokers.
- B. Recruitment and talent management systems we utilize in the job application process.
- C. Vendors providing services to the Company in connection with recruitment and job application processes, including providers of background checks, credit and consumer reporting agencies, and recruiters or staffing agencies.
- D. Consultants and vendors providing services to the Company regarding IT, cybersecurity, and privacy.

4. We May Use or Disclose Your Personal Information and Sensitive Personal Information for the Following Purposes:

4.1 The Personal Information and Sensitive Personal Information we collect, and our use of Personal Information and Sensitive Personal Information, may vary depending on the circumstances. We may use or disclose Personal Information and Sensitive Personal Information we collect from you or about you for one or more of the following purposes:

- (a) To fulfill or meet the purpose for which you provided the information. For example, if you disclose your name and contact information to apply for a job, we will use that Personal Information in connection with your candidacy for employment.
- (b) To use for our internal business operations and processes, including business and financial planning, analysis, recordkeeping, data management, security, and business continuity.
- (c) To comply with local, state, and federal law and regulations and/or to exercise other legal rights and comply with obligations.

- (d) To evaluate, make, and communicate decisions regarding your job application and candidacy for employment.
- (e) To obtain and verify background checks, references, and employment history.
- (f) To communicate with you regarding your candidacy for employment.
- (g) To evaluate and improve our recruiting methods and strategies.
- (h) To engage in lawful monitoring of job applicant activities and communications when they are on Company premises, or utilizing Company internet and Wi-Fi connections, computers, networks, devices, software applications or systems.
- (i) To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company related to recruiting or processing of data from or about job applicants.
- (j) To improve job applicant experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
- (k) To engage in corporate activities, obligations or transactions requiring review or disclosure of job applicant records subject to non-disclosure agreements.
- (l) To protect against malicious, unauthorized, or illegal activity and hold accountable those responsible.
- (m) To prevent identity theft.
- (n) To verify and respond to consumer requests under applicable consumer privacy laws.

4.2 We may disclose your personal information to the categories of third parties identified in Section 3 for the business purposes identified above.

4.3 We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration or share your personal information with third parties for cross-context behavioral advertising.

4.4 We do NOT and will not use or disclose your sensitive personal information for the purpose of inferring characteristics about you or for purposes other than those permitted by law.

4.5 We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect job applicants, our employees, or the public.

5. Retention of Personal Information

5.1 We will retain each category of personal information in accordance with our established data retention schedule. In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to the business purposes for which the Personal Information was collected; relevant federal, state, and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

5.2 We review our data retention policies and procedures regularly to determine if or when the business purposes and/or legal reasons for retaining the personal information are no longer applicable, in which case we arrange for the deletion or destruction of the personal information in a secure manner.

6. How We Protect the Information That We Collect

The protection of the information that we collect about job applicants is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- (a) We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- (b) We restrict access to private information to those who need such access in the course of their duties for us.

7. California Residents' Rights Regarding Personal Information

7.1 If you are a resident of California, you have the following rights pursuant to the CCPA, subject to the exceptions in such laws. To the extent such rights are otherwise authorized by other applicable state privacy laws, you may have the same or similar rights.

- (a) **Right to Know.** The right to request, up to 2 times in a 12-month period, that we identify to you: (i) the categories of personal information we have collected about you, (ii) the categories of sources from which the personal information was collected, (iii) the business purpose for which we use this information, and (iv) the categories of third parties with whom we disclose or have disclosed your personal information;
- (b) **Right to Access.** The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you;
- (c) **Right to Delete.** The right to request that we delete personal information that we have collected from you, subject to applicable exceptions;
- (d) **Right to Correct.** The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;
- (e) The right to designate an authorized agent to submit one of the above requests on your behalf (see below for how you can designate an authorized agent); and
- (f) The right to not be discriminated or retaliated against for exercising any of the above rights.

7.2 California residents (or other job applicants if applicable) may submit requests to exercise the above rights using the options below:

- (a) Submit a completed “**Employee/Job Applicant Exercise of Rights Request Form**” available for download at <https://careers.crestron.com/>.
- (b) Call our toll-free employee privacy support line at 1-888-885-2920.
- (c) Contact the Company at employeeprivacy@crestron.com.

7.3 How we will verify that it is really you who are submitting the request:

When you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide information sufficient to verify your identity. Specifically, we will ask you to verify information that we can use to link your identity to particular information in our possession.

7.4 Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct requests:

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessary information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is incorrect, unmerited, fraudulent, or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with your request.

7.5 If you have an authorized agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission, and documentation sufficient to demonstrate that they have been authorized by you to act on your behalf.

8. Changes to our California Job Applicant Privacy Policy and Notice

We may from time to time update this California Job Applicant Privacy Policy and Notice. If we make material changes to, we will notify you by posting the revised California Job Applicant Privacy Policy and Notice and the revised effective date on the Company's Careers webpage at:

<https://careers.crestron.com/>.

9. Individuals with Disabilities

This Notice is in a form that is or will be made accessible to individuals with disabilities.

10. Questions About the California Job Applicant Privacy Policy and Notice

If you have any questions about this Job Applicant Privacy Policy, please contact us at employeeprivacy@Crestron.com or call 1-888-885-2920.

