



COUNTY OF KINGS ELECTIONS DEPARTMENT

1-800-289-9981 ext. 4401 / 559-852-4401
FAX: (559) 585-8453

Lupe Villa
Registrar of Voters
1400 W. Lacey Blvd. Bldg. #7
Hanford California 93230
Elections@CountyofKings.com

APPLICATION FOR VOTER REGISTRATION INFORMATION

This Application is made pursuant to California Elections Code §2188. It consists of six (6) pages and includes a Use Agreement as an integral part. It must be completed to the satisfaction of the Kings County Registrar of Voters and payment for Voter Registration Information received at the time the application is returned. The information provided is subject to verification. This Application shall be submitted in person or by U.S. Mail or other delivery/courier service. Responses must be printed or typed. **Applications that are emailed or faxed will not be accepted.** The Elections Department will not provide technical support for interpreting data. **The Elections Department will require a minimum of 3-5 business days to process the data once an application is approved.** Applications will be processed on a first come first served basis.

Applicant's Full Name		Name of Organization / Committee / Candidate / Campaign		
Email Address		Phone Number		
Applicant's Home Address		City	State	Zip
Organization Business Address		City	State	Zip
Voter Information				
<input type="checkbox"/> Voter File* – \$13.95 This file contains voter information such as names, addresses, contact information (if provided). Voter History can be added for an additional fee. File is available in digital .txt format only.				
<input type="checkbox"/> Walking List* – \$13.95 This file contains voter information such as names, addresses, and contact info (if provided) formatted in an easy-to-read list. Voter History can be added for additional fee. File is available in paper (a per page fee will be applied) or digital format.				
<input type="checkbox"/> Voter Labels* – The Elections office can generate a labels report for your use to mail out information. The fee is \$.03 cents per label. We can print the labels in office however an additional cost of \$2.05 per page will be incurred.				
<input type="checkbox"/> Candidate Contact List – \$3.25 This list provides the contact information for current candidates who have filed for the current election. This information is taken from their candidate paperwork. A list of current candidates is available on our website. Each list must be purchased separately (if applicable).				
*Please specify if you would like countywide data, specific district(s), or specific precinct(s):				
<input type="checkbox"/> Countywide <input type="checkbox"/> District(s): _____ <input type="checkbox"/> Area(s) if applicable: _____				
<input type="checkbox"/> Include Voter History (Not available on all reports. An additional \$3.25 per election will be assessed.):				
<input type="checkbox"/> Past 5 Elections <input type="checkbox"/> Election Date(s)(maximum of 5) _____				
Would you like to designate a specific Political Party (check only ONE)? <input type="checkbox"/> All Parties <input type="checkbox"/> Rep <input type="checkbox"/> Dem <input type="checkbox"/> AI <input type="checkbox"/> Green <input type="checkbox"/> P&F <input type="checkbox"/> LIB <input type="checkbox"/> NPP				
Data Extracts				
<input type="checkbox"/> Absentee Voter List Daily – \$5.55 per report. This list shows who has returned a VMB ballot each day. Only available during an active election. Please attach a calendar specifying the dates you wish to pull the report.				
<input type="checkbox"/> Absentee Voter List Cumulative - \$5.55 per report. This list shows all voters who have returned a VBM ballot for the election. Only available during an active election.				
<input type="checkbox"/> Challenged Voter list. Missing Signature – \$5.55 This list contains the names of voters who did not sign their ballot return envelope.				
<input type="checkbox"/> Challenged Voter list. Non-matching Signatures - \$5.55 This list contains the names of voters whose signatures were challenged as not matching.				
<input type="checkbox"/> Precinct to District Export - \$18.55 This is a list of what precincts are inside of a district. The file is available in digital format only.				
Other Requests (Explain in detail below. Attach additional sheets if necessary)				
Choose Format: <input type="checkbox"/> Paper Report (not available for all reports. A per page fee of \$2.05 will be incurred.) <input type="checkbox"/> Digital Report				
Delivery Options Digital: <input type="checkbox"/> E-mail (via a secure website) <input type="checkbox"/> In-Person Flash Drive (a \$5.00 fee for the drive will be assessed.)				
Delivery Options Paper: <input type="checkbox"/> In Person <input type="checkbox"/> Certified Mail – A 9.00 fee will be assessed. Provide Mailing Address below:				

What type(s) of business, organization, or committee do you represent?

- Political
 Investigative
 Vendor
 Legal
 Initiative/Referendum
 Educational
 Governmental
 Recall Effort
 Media
 Other: _____

Provide the purpose of the request. A copy of your ID must be submitted with all requests.

Election Related purposes (Please check one of the boxes. Be sure the Organization name and business contact info is included on the first page.):

- Candidate or Proposed Ballot Measure
 Initiative / Referendum
 Recall
 Political Survey / Fundraising

Political Related Communications (documentation establishing compliance with section CCR 19003(a)(4), for example a letter establishing an affiliation with a political organization, is required).

Scholarly Research (a letter from the representative of the institution [professor, administrator, etc.] on the institution's letterhead stating that the applicant is authorized to receive the information, is required).

Journalistic Purposes (a clear copy of the applicant's press pass or media credential is required. In the event the applicant does not have a press pass or media credential, the applicant shall submit other evidence that they are a journalist.)

- Governmental Use
 Data Vendor Use
 Records Review
 (Permissible use is listed under California Code of Regulations Title 2, Division 7, Chapter 1, Article 1 § 19003.)

All requests for voter information shall be evaluated for compliance with Elections Code / Government Code by the Elections Office.

Explain in detail your intended use of this information and how you will keep it secure. Please attach additional sheets if more space is needed. For a request of specific voter registration records, provide detailed identifying information on the specific voter(s) here. You may request up to 10 specific voter registration records per application. Please attach sheets of paper if more space is needed. (2 CCR § 19008(a)(11), 19010)

AGREEMENT: All information furnished on this application is subject to verification.

_____ Initial	Applicant and beneficiary, if applicable, hereby agree that the information set forth in the voter registration records will be used only for approved purposes, consistent with state law, as defined by California Elections Code section 2194, California Code of Regulations section 19003, and United States Government Code § 6254.4.
_____ Initial	Applicant and beneficiary, if applicable, further agree not to sell, lease, loan, or deliver possession of the registration information, or a copy thereof, or any portion thereof, in any form or format, to any person, organization, or agency without first submitting a new application and receiving written authorization from the County of Kings to release such registration information.
_____ Initial	Applicant and beneficiary, if applicable, agree to maintain information in a secure and confidential manner using the best practices identified in Section 19012 of the California Code of Regulations Title 2, and will notify the Secretary of State immediately of any violation, exposure, and/or breach of voter registration information or suspected violation, exposure, and/or breach of voter registration information and will cooperate with the Secretary of State's office or any investigative agency efforts related to any resulting investigation. A copy of the document "Minimizing Cyber Risks" has been provided to the applicant.
_____ Initial	Applicant and beneficiary, if applicable, understand that it is a misdemeanor for a person in possession of voter registration information to use or permit the use of all or any part of the information for any purpose other than as permitted by law. (California Elections Code §18109)
_____ Initial	Applicant and beneficiary, if applicable, agree to pay the State of California, as compensation for any unauthorized use of each individual's registration information, a penalty as described in California Code of Regulations Section 19007. A copy of relevant California Codes of Regulations along with relevant California Election code has been provided to the applicant.

I CERTIFY UNDER PENALTY OF PERJURY, UNDER THE LAWS OF THE STATE OF CALIFORNIA, THAT ALL OF THE INFORMATION PROVIDED BY ME WITHIN THIS APPLICATION IS TRUE AND CORRECT.

Signature of Applicant or Agent:	Date:
Name of Applicant or Agent (Print):	Drivers License or State ID Number:

Place of application execution:

- CLEAR COPY OF APPLICANT'S PHOTO ID PROVIDED
 COPY OF PRESS PASS / MEDIA CREDENTIALS PROVIDED (IF APPLICABLE)

FOR OFFICE USE ONLY

<input type="checkbox"/> Approved <input type="checkbox"/> Denied	Date Requested	Date Completed	Amount Paid	Verified By
---	----------------	----------------	-------------	-------------

VOTER FILE CODES AND REGULATIONS: PERMISSIBLE AND NON-PERMISSIBLE ACCESS TO VOTER REGISTRATION

**California Code of Regulations Title 2, Division 7, Chapter 1, Article 1:
Access to Voter Registration Information**

19002. Application of this Article.

a) This Article shall apply to any person who directly or indirectly receives voter registration information from any source agency.
 b) This Article shall not apply to any voter requesting their own voter registration information through a publicly available voter record lookup tool. However, when a voter requests additional information about their own specific voter record than is available on such a tool, they must submit an application for specific voter registration record pursuant to this Article.

19003. Permissible Uses.

(a) Voter registration information obtained from a source agency shall be used solely for the following purposes:

(1) Election: for any person to communicate with voters in connection with an election by means that shall include, but shall not be limited to, the following:

- (A) Communicating with voters for or against any candidate or ballot measure in any election;
 - (B) Communicating with voters regarding the circulation or support of, or opposition to, any recall, initiative, or referendum petition;
 - (C) Surveying voters in connection with any specific election campaign or specific potential election campaign in which any voter registered to vote may vote;
 - (D) Surveying voters in connection with an election-related exploratory committee;
 - (E) Soliciting contributions or services as part of any election campaign on behalf of any candidate for public office or any political party or in support of or opposition to any ballot measure, initiative, or referendum petition.
- (2) Scholarly: students working on theses, professors researching voting patterns, and other academics involved in research related to political or election activities.
- (3) Journalistic: members of the press for any purpose related to political or election activities.
- (4) Political: for any person to communicate with voters to influence public opinion related to political or election activities. The content of such communications shall include, but shall not be limited to: news and opinions of candidates, elections, education related to political matters, political party developments, ballot measures, initiatives, referendum positions, and related political matters.

(5) Governmental: Any request from a governmental agency or for a use related to a governmental function by means including, but not limited to:

- (A) Encouraging participation in the United States Census;
- (B) Conducting any survey of opinions of voters by any government agency or its contractors;
- (C) Any official use by any local, state, or federal governmental agency, which shall include use in connection with any judicial proceeding or investigation involving or being conducted by any local, state, or federal governmental agency.
- (6) Record review: For any person to conduct an audit of voter registration lists for election, scholarly, journalistic, political, or governmental purposes. Record review includes, but is not limited to, detecting voter registration fraud, evaluating voter registration information accuracy, and evaluating compliance with applicable Federal and California laws.

(7) Vendor: By any vendor to compile and/or organize voter registration information for another person's use consistent with this Article.

(b) Requests for voter registration information for a purpose not specifically listed in subdivision (a), and not prohibited by section 19004, shall be evaluated for compliance with the Elections Code by the source agency.

(c) A source agency shall review each application for compliance with the Elections Code and this Article independent of decisions made on other applications.

19004. Impermissible Uses.

(a) Using voter registration information in a manner contrary to the authorized uses specified in Elections Code section 2194 is impermissible. Impermissible uses include, but shall not be limited to:

- (1) Any communication for any personal, private, or commercial purpose other than for those purposes permitted by Section 19003.
- (2) Solicitation of contributions or services for any personal, private, or commercial purpose.
- (3) Conducting any survey of opinions of voters other than for those purposes permitted by Section 19003, subdivision (a).
- (4) Using the voter registration information to harass any voter or the voter's household, including, but not limited to, any conduct prohibited by Elections Code sections 18540 and 18543.
- (b) Voter registration information shall not be sent outside of the United States, as specified in Elections Code section 2188.5.
- (c) Notwithstanding section 19003, a source agency may reject a request for voter registration information based on a reasonable belief or determination that it is being requested for use in a manner prohibited by law, including, but not limited to, uses contrary to the prohibitions or authorized uses specified in Elections Code sections 2188.5 and 2194 or that is contrary to Elections Code section 10. An impermissible purpose may include requests for voter registration information for an impermissible

set forth in the voter registration information will be used for the approved purposes, consistent with state law, as defined by Elections Code section 2194, this Article, and Government Code section 6254.4.

purpose-submitted for fraudulent purposes or in bad faith or for the purpose of harassing or defrauding a person or entity. In such instances, the source agency shall provide the applicant its reasons for refusal. An applicant whose application is rejected shall not be prohibited from filing a new application.

19005. Transfers.

(a) Only a vendor may transfer voter registration information to another person, as described in subdivision (c).

(b) A beneficiary, including a vendor, may share voter registration information with their agent(s) without prior written authorization from a source agency.

(1) An agent may only use the voter registration information for the purposes specified in the approved application.

(2) A beneficiary sharing voter registration information with an agent must exercise reasonable care that the agent uses the voter registration only for purposes approved by the source agency and report any unauthorized use as described in Section 19012 of this Article.

(3) A beneficiary remains responsible for the actions of their agent with respect to the use of the voter registration information.

(c) A vendor may provide voter registration information to another person, other than its agent as described in subdivision (b), only upon providing written notification to the Secretary of State.

(1) This is intended to mean that the Secretary of State can approve the transfer of voter registration information obtained from both the Secretary of State and other source agencies.

(2) This notification shall include the name, address, phone number, and email address of the person to whom the information is provided. If applicable, the notification shall also include the business name and address of the person to whom the information is provided.

(3) A vendor that provides voter registration information to another person must share, in writing, the information security requirements in Section 19012 with that person and acknowledge, in writing, that they provided this information in the notification.

(4) A vendor who fails to provide the notification or transfers voter registration information to another person for an impermissible purpose shall be issued a warning by the Secretary of State for the first violation. For a second violation, a vendor will be barred from providing voter registration information to any person for the remainder of that presidential election cycle, defined as the period beginning on a presidential election day through the next presidential election day.

(5) This Article shall apply to any person who receives voter registration information from a vendor, as if that person had received the voter registration information directly from a source agency.

19008. Application.

(a) Every applicant shall execute and deliver to the source agency an application that contains all of the following information:

- (1) The full name of the applicant, and, if applicable, the full name of the beneficiary of the requested voter registration information.
- (2) The applicant's telephone and email address.
- (3) The applicant's complete business address.
- (4) The applicant's complete mailing address, if different from the business address.
- (5) If applicable, the complete business address of the beneficiary of the requested voter registration information.
- (6) The purpose(s) or type(s) of business, organization, or committee that the applicant represents.
- (7) The purpose(s) for which the request for voter registration information is made and the specific intended use(s) of this information or data in accordance with Section 19003.

(A) If the intended use of the requested voter registration information is for political purposes, the applicant shall submit documentation establishing compliance with section 19003(a)(4), for example a letter establishing an affiliation with a political organization.

(B) If the intended use of the requested voter registration information is for scholarly purposes, the applicant shall submit a letter from the representative of the institution (professor, administrator, etc.) on the institution's letterhead stating that the applicant is authorized to receive the information.

(C) If the intended use of the requested voter registration information is for journalistic purposes, the applicant shall submit a clear copy of the applicant's press pass or media credential. In the event the applicant does not have a press pass or media credential, the applicant shall submit other evidence that they are a journalist. The source agency shall determine whether submitted press passes, media credentials, or other evidence properly establish a journalistic purpose.

(8) A detailed explanation of how the requested voter registration information will be maintained securely and confidentially consistent with Section 19012.

(9) The type of information requested. Examples include voter history, precinct to district information, whether voter registration information is requested for a specific jurisdiction, and specific voter registration information.

(10) Shipping instructions for the source agency to deliver the requested voter registration information.

(11) If applicable, detailed identifying information on a specific voter for a request of a single voter's voter registration information.

(12) A completed agreement section, which contains spaces where the applicant must place their initials acknowledging the following statements:

- (A) Applicant and beneficiary, if applicable, hereby agree that the information
- (2) Apply security best practices, which includes the following:
 - (A) Obtain training on security awareness to avoid social engineering and

(B) Applicant and beneficiary, if applicable, further agree not to sell, lease, loan, or deliver possession of the registration information, or a copy thereof, in any form or format, to any person, organization, or agency except as prescribed in Section 19005.

(C) Applicant and beneficiary, if applicable, agree to maintain information in a secure and confidential manner using the best practices identified in Section 19010 of this Article, and will notify the Secretary of State immediately of any violation, exposure, and/or breach of voter registration information or suspected violation, exposure, and/or breach of voter registration information and will cooperate with the Secretary of State's office or any investigative agency efforts related to any resulting investigation.

(D) Applicant and beneficiary, if applicable, understand that it is a misdemeanor for a person in possession of voter registration information to use or permit the use of all or any part of the information for any purpose other than is permitted by law.

(E) Applicant and beneficiary, if applicable, agree to pay the State of California, as compensation for any unauthorized use of each individual's registration information, a penalty as described in Section 19007 of this Article.

(b) The applicant shall certify the content of the application as to its truthfulness and correctness, under penalty of perjury, with the applicant's signature and the date and place of signing.

19009. Application Submission and Processing.

(a) The applicant must submit the completed application for voter registration information in the following manner:

(1) The applicant must deliver it to the source agency in person or by U.S. mail or other delivery/courier service. A wet signature is required on the application; therefore, a source agency shall not accept emailed and faxed applications for voter registration information.

(2) The applicant must include a clear copy of their current photo identification issued by a federal or state government agency with the completed application.

(3) The applicant must submit the appropriate fee with the completed application.

(b) All source agencies, including the Secretary of State, shall process applications in the following manner:

(1) The source agency shall process requests for voter registration information in the order received.

(2) The source agency shall log all applications received, including whether each application was approved or denied and the contact information of each applicant, and maintain in this log all applications received, at a minimum, in the past five years.

(3) If the application is denied, the source agency shall inform the applicant of the reasons for denial, and shall return all application materials, including any payment. Payment will not be processed for denied applications.

(A) The Secretary of State shall inform the applicant of the reasons for denial in writing. Other source agencies may, but are not required to inform the applicant of the reasons for denial in writing.

(c) Applicants may re-submit denied applications after addressing the reason(s) for denial.

19010. Requests for Specific Voter Records.

(a) If specific voter registration record(s) are requested, the source agency shall only use the exact information provided by the applicant to locate the record(s). The applicant shall provide as much detail as is possible, including, but not limited to, the full name, date of birth, and present and/or former residence address of the specific voter that is the subject of the request.

(b) The source agency will only use the exact information provided (full name, date of birth, county of residence, and residence address, etc.) to identify specific voter registration record(s).

(c) In the event there are insufficient details for the source agency to fulfill the request for a specific voter registration record, the source agency shall communicate that fact to the applicant to determine if additional criteria to identify the voter(s) is available.

(d) If the request cannot be filled, the source agency shall send a letter to the applicant stating such. Payment will not be processed for requests that cannot be filled.

(e) An applicant may request up to 10 specific voter registration records per application. A variant of a name shall be considered a part of one request.

19011. End User Technical Support.

A source agency that provides voter registration information under this Article is not responsible for end-user technical support for processing purchased data or for assistance on converting provided data for usage.

19012. Requirements for Storage and Security of Voter Registration Information.

(a) Any person who has directly or indirectly obtained voter registration information from a source agency must exercise due diligence in maintaining and securing the voter registration information in order to reduce the risk of information exposure and/or breach.

(b) Any person who has directly or indirectly obtained voter registration information from a source agency shall:

(1) Use a strong and unique password ("strong password hygiene") per account with access to the voter registration information or privileges to grant access.

Who Face Threats or Violence Because of Work for a Public Entity program pursuant to Chapter 3.2 (commencing with Section 6215) of Division 7 of Title 1 of the Government Code.

California Elections Code § 2166.7 (Not Full Text)

If authorized by the county board of supervisors, a county elections official shall, upon application of a public safety officer, make confidential that

phishing attacks.

(B) Practice the principles of "least privilege" by restricting user access to the minimum need based on users' job necessity.

(C) Ensure user accounts are logged off or the session is locked after a period of inactivity, which shall be no more than 15 minutes.

(D) Remove, deactivate, or disable accounts or default credentials.

(E) Erase or wipe voter registration information that is no longer needed for its retention and sanitized following National Institute of Standards and Technology (NIST) 800-88 Guidelines for media sanitization.

(F) Restrict physical access by not leaving your computer in places unlocked and unattended.

(G) Limit the use of portable devices. If a portable device is used, strong storage encryption procedures must be applied utilizing Federal Information Processing Standards (FIPS) 197, commonly referred to as "Advanced Encryption Standard" or "AES."

(H) Use wireless technology securely with Wi-Fi Protected Access 2 (WPA2) or better.

(c) In addition to the requirements set forth in (b) above, any vendor shall:

(1) Apply additional security best practices, which include the following:

(A) Use strong identity and access management, preferring multi-factor authentication for any and all privilege accounts and/or accounts with access to voter registration data.

(B) Initiate an account lockout after a pre-defined number of failed attempts, no more than 10. Any automated account unlock actions must wait no less than 30 minutes from the lockout event.

(C) Force password changes on a pre-defined basis, but not less than 365 days.

(D) Backups of voter registration information shall be securely stored separately and utilizing FIPS 197 encryption at rest.

(2) Implement security log management, which includes the following:

(A) Enable logging on all systems and network devices with sufficient information collection that answers the following:

(i) What activity was performed?

(ii) Who or what performed the activity, including where or on what system the activity was performed?

(iii) What activity was the action performed on?

(iv) What tool(s) were used to perform or performed the activity?

(v) What was the status, outcome, or results of the activity?

(B) Review log(s) regularly for any errors, abnormal activities and any system configuration changes.

(C) Securely store log files separately from the systems monitored, archived, and protect from unauthorized modification, access, or destruction.

(D) Use log monitoring tools to send real-time alerts and notifications.

(E) Utilize multiple synchronized United States-based time sources.

(3) Employ system hardening techniques, which include the following:

(A) Update and install all firmware and patches from a trusted and verifiable source.

(B) Use only the most up-to-date and certified version of vendor software.

(C) Install and maintain active malware and anti-virus software.

(D) Implement firewalls, also known as host-based firewalls, and/or port filtering tools with host-based intrusion protection services.

(E) Encrypt voter registration information using FIPS 197 at rest.

(F) Encrypt voter registration information in transit such as Transport Layer Security (TLS) 1.2 or better with a valid certificate and certificate chain.

(G) Do not use self-signed certificates.

(H) Conduct regular vulnerability scanning and testing for known or unknown weaknesses.

(I) Use application whitelisting on all endpoints and systems.

19013. Reporting Requirement for Unauthorized Use and Data Breaches.

Any person who has obtained voter registration information from a source agency shall report detected unauthorized use, suspected breach, or denial of service attack on the voter registration information or the system containing the voter registration information to the Secretary of State Elections Division Help Desk within twenty-four (24) hours of discovery.

California Elections Code § 2166 (Not Full Text)

(a) Any person filing with the county elections official a new affidavit of registration or reregistration may have the information relating to his or her residence address, telephone number, and email address appearing on the affidavit, or any list or roster or index prepared therefrom, declared confidential upon order of a superior court issued upon a showing of good cause that a life-threatening circumstance exists to the voter or a member of the voter's household, and naming the county elections official as a party.

California Elections Code § 2166.5 (Not Full Text)

(a) Any person filing with the county elections official a new affidavit of registration or reregistration may have the information relating to their residence address, telephone number, and email address appearing on the affidavit, or any list or roster or index prepared therefrom, declared confidential upon presentation of certification that the person is a participant in the Address Confidentiality for Victims of Domestic Violence, Sexual Assault, and Stalking program pursuant to Chapter 3.1 (commencing with Section 6205) of Division 7 of Title 1 of the Government Code, or a participant in the Address Confidentiality for Reproductive Health Care Service Providers, Employees, Volunteers, Patients, and Other Individuals

California Election Code § 18109. Misuse of information: Misdemeanor.

(a) It is a misdemeanor for a person in possession of information identified in Section 2138.5, or obtained pursuant to Article 5 (commencing with Section 2183) of Chapter 2 of Division 2 of this code or Section 7924.000 of the

officer's residence address, telephone number, and email address appearing on the affidavit of registration, in accordance with the terms and conditions of this section.

California Elections Code § 2188. Application for Voter Registration Information.

- (a) Any application for voter registration information available pursuant to law and maintained by the Secretary of State or by the elections official of any county shall be made pursuant to this section.
- (b) The application shall set forth all of the following:
- (1) The printed or typed name of the applicant in full.
 - (2) The complete residence address and complete business address of the applicant, giving street and number. If no street or number exists, a postal mailing address as well as an adequate designation sufficient to readily ascertain the location.
 - (3) The telephone number of the applicant, if one exists.
 - (4) The number of the applicant's driver's license, state identification card, or other identification approved by the Secretary of State if the applicant does not have a driver's license or state identification card.
 - (5) The specific information requested.
 - (6) A statement of the intended use of the information requested.
- (c) If the application is on behalf of a person other than the applicant, the applicant shall, in addition to the information required by subdivision (b), set forth all of the following:
- (1) The name of the person, organization, company, committee, association, or group requesting the voter registration information, including their complete mailing address and telephone number.
 - (2) The name of the person authorizing or requesting the applicant to obtain the voter registration information.
- (d) The elections official shall request the applicant to display his or her identification for purposes of verifying that identifying numbers of the identification document match those written by the applicant on the application form.
- (e) The applicant shall certify to the truth and correctness of the content of the application, under penalty of perjury, with the signature of his or her name at length, including given name, middle name or initial, or initial and middle name. The applicant shall state the date and place of execution of the declaration.
- (f) Completed applications for voter registration information shall be retained by the elections official for five years from the date of application.
- (g) This section shall not apply to requests for information by elections officials for election purposes or by other public agencies for governmental purposes.
- (h) The Secretary of State may prescribe additional information to be included in the application for voter registration information.
- (i) A county may not provide information for any political subdivision that is not wholly or partially contained within that county.

California Elections Code § 2188.5

- (a) A person who requests voter information pursuant to Section 2188 or who obtains signatures or other information collected for an initiative, referendum, political party qualification, or recall petition shall not send that information outside of the United States or make it available in any way electronically to persons outside the United States, including, but not limited to, access over the Internet.
- (b) For purposes of this section, "United States" includes each of the several states of the United States, the District of Columbia, and the territories and possessions of the United States.

California Election Code § 2194 (Not Full Text)

- (a) Except as provided in Section 2194.1, the affidavit of voter registration information identified in Section 7924.000 of the Government Code:
- (1) Shall be confidential and shall not appear on any computer terminal, list, affidavit, duplicate affidavit, or other medium routinely available to the public at the county elections official's office.
 - (2) Shall not be used for any personal, private, or commercial purpose, including, but not limited to:
 - (A) The harassment of any voter or voter's household.
 - (B) The advertising, solicitation, sale, or marketing of products or services to any voter or voter's household.
 - (C) Reproduction in print, broadcast visual or audio, or display on the internet or any computer terminal unless pursuant to paragraph (3).
 - (3) Shall be provided with respect to any voter, subject to the provisions of Sections 2166, 2166.5, 2166.7, and 2188, to any candidate for federal, state, or local office, to any committee for or against any initiative or referendum measure for which legal publication is made, and to any person for election, scholarly, journalistic, or political purposes, or for governmental purposes, as determined by the Secretary of State.
 - (4) May be used by the Secretary of State for the purpose of educating voters pursuant to Section 12173 of the Government Code.

Government Code, knowingly to use or permit the use of all or any part of that information for any purpose other than as permitted by law.

(b) It is a misdemeanor for a person knowingly to acquire possession or use of voter registration information from the Secretary of State or a county elections official without first complying with Section 2188.

California Government Code Title 1, Division 10, Part 5, Chapter 2, Article 1: Voter Information

- (a) Except as provided in Section 2194 of the Elections Code, both of the following are confidential and shall not be disclosed to any person:
- (1) The home address, telephone number, email address, precinct number, or other number specified by the Secretary of State for voter registration purposes.
 - (2) Prior registration information shown on an affidavit of registration.
- (b) The California driver's license number, the California identification card number, the social security number, and any other unique identifier used by the State of California for purposes of voter identification shown on an affidavit of registration, or added to the voter registration records to comply with the requirements of the federal Help America Vote Act of 2002 (52 U.S.C. Sec. 20901 et seq.), are confidential and shall not be disclosed to any person.
- (c) The signature of the voter that is shown on an affidavit of registration is confidential and shall not be disclosed to any person.
- (d) For purposes of this section, "home address" means street address only, and does not include an individual's city or post office address.

Minimizing Cyber Risk – Receiving a Confidential Voter File

You are receiving voter information from the County of Kings, California. Please note that the provided information is confidential and may be used for election, scholarly, journalistic, political, or governmental purposes only. Please be aware that you are responsible for keeping this information secure.

Political parties, candidates and elections administrators cannot be alone in the fight against malicious actors who seek to undermine our elections. As political campaigns and organizations are targets of cyber threats, they too have a role and responsibility in defending our democracy. Your actions are critical in maintaining public trust in our elections and minimizing the threat of cyber incidents.

As an integral part of protecting our democracy, we wish to remind you to take preventative measures to reduce the likelihood and severity of cyber incidents.

Recognized best practices for minimizing risk:

1. Obtain training on security awareness to avoid social engineering and phishing attacks.
2. Practice the principles of “least privilege” by restricting user access to the minimum need based on users’ job necessity.
3. Ensure user accounts are logged off or the session is locked after a period of inactivity, which should be no more than 15 minutes.
4. Remove, deactivate, or disable accounts or default credentials.
5. Erase or wipe voter registration information that is no longer needed for its retention and sanitize following National Institute of Standards and Technology (NIST) 800-88 Guidelines for media sanitization.
6. Restrict physical access by not leaving your computer in places unlocked and unattended.
7. Limit the use of portable devices. If a portable device is used, strong storage encryption procedures must be applied utilizing Federal Information Processing Standards (FIPS) 197, commonly referred to as “Advanced Encryption Standard” or “AES.”
8. Use wireless technology securely with Wi-Fi Protected Access 2 (WPA2) or better.
9. Use a strong and unique password (“strong password hygiene”) per account with access to the voter registration information or privileges to grant access.

If you detect suspicious activity:

In the event you observe or detect any suspicious activity, please alert law enforcement officials immediately and contact the Kings County Elections office or the California Secretary of State’s office with any important information. As a reminder, California state law requires any entity that has access to voter data from the California Secretary of State’s office to report a breach of this information to the appropriate officials as quickly as possible.