CALIFORNIA ENTERPRISE DEVELOPMENT AUTHORITY

a CALED sponsored organization

POLICY AND PROCEDURE

ELECTRONIC MEDIA POLICY

Adopted by the CEDA Board of Directors, November 15, 2018

I. PURPOSE

The employees of the California Enterprise Development Authority ("Authority") use various forms of electronic media including, but not limited to, computers, email, telephones, facsimiles, copy machines, Internet, personal data devices (PDAs), and other devices capable of sending, receiving, and accessing various types of communications in the commission of their regularly assigned duties and responsibilities. As used herein, the term "employee" or "employees" shall include employees hired directly by the Authority as well as employees of the California Association for Local Economic Development who perform work for the Authority pursuant to a written agreement. This policy establishes procedures for the use of such communication devices including all software, databases, hardware, and digital files which are the property of the Authority.

Employees should have no expectation of privacy with regard to Authority electronic communication, whether it is made on an Authority device or personal device used for Authority purposes. The Authority has a right to access and inspect all Authority electronic communications and devices at any time. All Authority communications and records, regardless whether they are maintained on an Authority or personal device, may be subject to disclosure under a California Public Records Act ("CPRA") request.

II. POLICY

This policy establishes minimum standards for all Authority employees.

1. Authority electronic communications and media shall not be used in any manner that would be discriminatory, harassing or obscene, or for any other purpose that is illegal, in violation of Authority policy or may damage the reputation of the Authority.

2. Employees shall not install personal software on an Authority computer system or device.

3. All electronic information created by any employees using any means of Authority electronic communications is the property of the Authority and remains the property of the Authority.

4. Personal passwords may be used for purposes of security, but the use of a personal password does not affect the Authority's ownership of the electronic information. The Authority may override all personal passwords, if necessary, for any reason.

5. The Authority reserves the right to access and review electronic files, email messages, text messages, telephone messages, mail, and digital archives. The Authority also reserves the right to monitor the use of Authority electronic communications, as necessary, to ensure that no misuse or violation of Authority policy or law occurs.

6. Employees are not permitted to access the electronic communications of other employees or third parties unless directed to do so by Authority management.

7. No employee shall install or use anonymous or personal email transmission programs or encryption of email communications, except as specifically authorized by Authority management.

8. Access to the Internet, websites, and other types of Authority authorized communication software (e.g., email) is to be used for Authority related business only.

9. Employees shall only send emails or other electronic communication regarding Authority business using Authority issued or approved communication media or devices.

10. Employees shall not use Authority web pages for personal or commercial reasons and shall not establish any links to the Authority's website without the Authority's approval.

11. Employees shall not copy or download data or programs for personal or commercial use from any Authority computer, device, program or Internet access.

12. No personal electronic communication device shall be connected to the Authority's network without prior Authority approval.

13. Personal use of Authority facsimile and copy machines should be minimal.

14. Personal phone calls using Authority telephones should be minimal. The Authority shall be reimbursed for any long distance or other charges resulting from personal phone calls.

15. All text-based communication, including email, is subject to the Authority's record retention policies and procedures. This includes Authority communications and records retained on a personal communication device.

16. All text-based communication, including email, containing information related to Authority business may be subject to disclosure under a CPRA request. This includes communications made, received, or retained on Authority or personal mobile electronic devices used for Authority purposes.

17. Employees are required to conduct a good faith search of any Authority records responsive to a CPRA request. The search will include inspection of all of the employee's Authority and personal accounts and devices that are used to conduct Authority business.

III. REVIEW OF DEVICES IN RESPONSE TO A CALIFORNIA PUBLIC RECORDS ACT REQUEST

Upon receipt of a CPRA request, Authority management will identify employees who may have responsive documents. Those employees are required to search for documents in response to a CPRA request in good faith. The employee's search will include Authority devices and accounts and any personal accounts and devices the employee uses to conduct Authority business. The employee alone will be responsible for searching his or her personal accounts and devices. To comply with the law and to protect the privacy of its employees, the Authority will take the following steps:

1. Identify the employee(s) who may have documents relevant to the request.

2. Communicate the scope of the request to those employees.

3. Request that the employee(s) search his or her personal files, accounts, and devices for materials responsive to the request.

4. If an employee(s) wants to withhold documents that could be potentially responsive to the request, the employee may submit an affidavit to the Authority and a reviewing court, if applicable, that states why the documents are a personal record and not a public record.

IV. ACCOUNTABILITY

Employees violating this policy are subject to disciplinary action.

All Authority employees are required to read and familiarize themselves with the Electronic Media Policy and the Mobile Electronic Device and Use Policy. Because changes or modifications may be made to these policies as technology evolves, it is

each employee's responsibility to periodically review the policies to ensure compliance with the most current requirements.

I acknowledge receipt of this policy and understand and agree that I am bound by its contents:

_____ _____

Employee Signature Date