

Memorandum of Understanding
between the
All Faculty Association
and
Sonoma County Junior College District
regarding

Article 31: Electronic Security Systems

April 22, 2020

AFA and the District agree to the following changes to Art. 31: Working Conditions.

31.09 ELECTRONIC SECURITY SYSTEMS: The purpose of this section is to identify parameters for the use of electronic security systems that effectively address AFA and the District's mutual interest in fostering a safe workplace and educational environment, while respecting and protecting the privacy and academic freedom of faculty members. For purposes of this section, electronic security systems shall mean any electronically based technology that enables identification of the location and/or actions of specific persons at specific times. AFA and the District agree to negotiate language that is generally applicable to any form of surveillance and that articulates the principles supporting the provisions of §31.09, specifically, the importance of maintaining a safe workplace and protecting the faculty from all forms of malignant and invasive surveillance, regardless of the technology employed. AFA and the District further agree to negotiate the terms implicated by the utilization of specific new technologies.

A. **Approved Purposes:** The following are the sole approved purposes for the use of electronic security systems.

1. Protecting life and property.
2. Assisting in the investigation of a violation of law.

B. **Limitations on Placement of Electronic Security Systems**

1. **Security Camera Notification:** The District shall reasonably locate clear signage providing notice that an area is monitored by a security camera.
2. **Prohibition of Location:** Electronic security systems shall neither be placed in, nor directed into, classrooms, faculty offices, conference rooms, restrooms, break rooms and other areas where faculty members regularly engage in professional duties and/or have a reasonable expectation of privacy.
3. **Changes to Locations Monitored by Electronic Security Systems:** The District shall provide AFA with a listing of the current locations monitored by electronic security systems. The District shall provide AFA with written notice of any proposed change in locations monitored by security cameras or key-card-enabled door locks no less than thirty (30) business days in advance of making the proposed change. AFA may, within twenty (20) business days of receiving such notice, demand to meet and confer with the District if it believes the proposed change violates this Article or requires further impacts bargaining prior

to implementation. Within ten (10) business days after the meet and confer process is completed, the District shall provide AFA with written notice whether it intends to proceed with the proposed change. AFA shall not file a grievance or other action asserting violation of this Article by the proposed change without first utilizing the meet and confer process afforded by this subsection. The District shall not proceed with the proposed change under this subsection during the meet and confer and/or grievance process.

4. **Limits on technology:** Monitoring technologies used by District electronic security systems are limited to video security cameras and key-card-enabled door locks. Storage and/or analysis by a third party of any portion of the data obtained by District electronic security systems is prohibited. The use of facial recognition technology is prohibited.

C. **Limitations on Access to Data:** Consistent with the approved purposes set forth in 31.09.A, data recorded by electronic security systems shall be accessed only under the following circumstances:

1. The District, through its Chief of Police (or designee), has probable cause that a violation of law has occurred and that access to the data would assist in the formal investigation.
2. Subject to a lawful subpoena, judicial order, or other legal obligation to produce the data to a third party.
3. As a result of an insurance investigation.

D. **Limitations on District Use of Data Accessed from Electronic Security Systems**

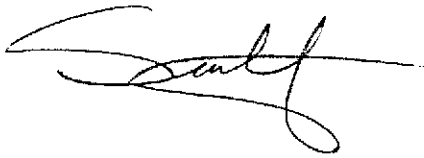
1. **Prohibition of Use for Reviewing and Evaluating Members' Performance.** Data gathered from electronic security systems shall not be used to monitor faculty members' attendance, work or work habits, nor shall such information be used in any part of the evaluation process.
2. **Limited, Permissible Use for Disciplinary Purposes.** Data accessed from an electronic security system shall not be used as evidence in a disciplinary action against a faculty member, unless that action specifically involves a violation of law.

E. **Authorized Access:** When one or more of the circumstances described in 31.09.C has prompted a request for data from an electronic security system to be examined or disclosed, the following shall apply:

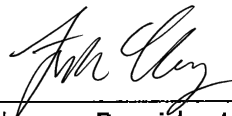
1. **Authorization:** Except for when required by law or in emergencies, access to data must be authorized in advance and in writing by the President or appropriate Vice President. The President or appropriate Vice President shall ensure that the request to access data complies with this Article.
2. **Required by Law:** When the District receives a search warrant, subpoena or other legally required request of electronic security system data, the data may be preserved immediately without authorization, but appropriate authorization for access must then be sought as soon as legally permissible.
3. **Emergencies:** In emergencies, the least perusal of data and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay. Emergencies are defined as when time is of the essence and there is a high probability that delaying action would almost certainly result in significant bodily

harm, significant property loss, damage to the District or its assets, or loss of significant evidence of one or more alleged violations of law.

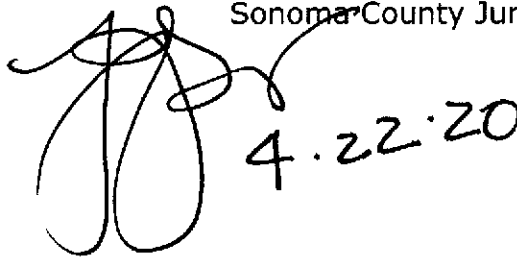
4. **District Police:** This Article does not preclude the District Police department from accessing data in an investigation into a possible criminal violation of law.
5. **Retention:** Electronic security system data shall be retained for a period of no more than ninety (90) calendar days from the time of recording, unless the data is accessed within that period for an approved purpose consistent with this Article, in which case the data shall be retained as long as required by applicable law.



Sean Martin, President
All Faculty Association



Dr. Frank Chong, President/Superintendent
Sonoma County Junior College District



4.22.20