

College Coordinating Council Meeting

Wednesday, March 13, 2019

A124 – President's Conference Room 9:00 a.m. – 10:00 a.m.

Type of Meeting: Regular Note Taker: Patty McClure

Please Review/Bring: Agenda, Minutes

Committee Members:

Van Rider, Academic Senate

VACANT, Associated Student Organization

Ed Knudson, President

Pamela Ford, Classified Union

Michelle Hernandez, Confidential/Management/Supervisory/Administrators

LaDonna Trimble, Deans Dr. Scott Lee, Faculty Union

VACANT, Vice President of Academic Affairs

Mark Bryant, Vice President of Human Resources

Dr. Erin Vines, Vice President of Student Services

		AGEN	DA	
	Items	Person(s)	Time	Action
		Responsible		
STANDIN				
l.	Approval of Previous Minutes of	All		
	February 13, 2019.			
II.	Constituent Reports	All		
INFORMA	TION/DISCUSSION/ACTION ITEMS:			
III.	AP 3720 – Computer, Network	Rick	3	Returned from November 14, 2018 CCC
	and Telecommunications Use		minutes	Meeting.
IV.	AP 3721 – Virtual Private Network	Rick	3	Returned from November 14, 2018 CCC
	(VPN)/Remote Access Procedure		minutes	Meeting.
V.	AP 3722- Acceptable Use	Rick	3	Returned from November 14, 2018 CCC
	Agreement		minutes	Meeting.
VI.	AP 6200 – Budget Preparation	Diana	5	Returned from November 14, 2018 CCC
			minutes	Meeting.
VII.	BP 6250 – Budget Management	Diana	5	Returned from January 9, 2019 CCC
	-		minutes	Meeting.
VIII.	BP & AP 6975 – Export Control	Diana	5	
	·		minutes	
IX.	AP 4230 – Grading and Academic	Erin	5	Returned from the January 9, 2019 CCC
	Record Symbols		minutes	Meeting.
X.	AP 5010 – Admissions	Erin	5	Returned from the January 9, 2019 CCC
			minutes	Meeting.
XI.	AP 5012 – International Students	Erin	5	Returned from the January 9, 2019 CCC
			minutes	Meeting.

XII.	AP 5031 – Instructional Material	Erin	5	Returned from the January 9, 2019 CCC
	Fees		minutes	Meeting.
XIII.	BP 2330 – Quorum and Voting	Ed/Mark	2	Revised from February 13, 2019 CCC
			minutes	Meeting.
XIV.	BP 2720 – Communications	Ed/Mark	2	Revised from February 13, 2019 CCC
	Among Board Members		minutes	Meeting.
XV.	BP 3900 – Speech: Time, Place	Ed/Mark	2	Revised from February 13, 2019 CCC
	and Manner		minutes	Meeting.
XVI.	Enrollment Management	LaDonna	5	
	Committee Composition		minutes	
FUTURE A	AGENDA ITEMS:			
NEXT N	MEETING DATE:			
	March 27, 2019			
	•			



College Coordinating Council Minutes

Wednesday, February 13, 2019

A124 – Foundation Conference Room 9:00 a.m. – 10:00 a.m.

Type of Meeting: Regular Note Taker: Patty McClure

Please Review/Bring: Agenda, Minutes

Committee Members:

Van Rider, Academic Senate

Allison Ammy, Associated Student Organization - ABSENT

Ed Knudson, President - **ABSENT** Pamela Ford, Classified Union

Michelle Hernandez, Confidential/Management/Supervisory/Administrators

LaDonna Trimble, Deans Dr. Scott Lee, Faculty Union

Vacant, Vice President of Academic Affairs

Mark Bryant, Vice President of Human Resources Dr. Erin Vines, Vice President of Student Services

		MINUT	TES	
	Items	Person(s) Responsible	Time	Action
STANDIN	IG ITEMS:			
I.	Approval of Previous Minutes of January 9, 2019.	All		The minutes were approved as presented.
II.	Constituent Reports	All		There were no reports.
INFORMA	ATION/DISCUSSION/ACTION ITEMS:			
III.	AP 5020 – Non Resident Tuition	Erin	2 minutes	Dr. Vines requested the item be pulled as there was new information and another revision needs to be done. This will return to another CCC meeting.
IV.	BP 2315 – Closed Sessions	Ed	2 minutes	There was some discussion on the clarification of the references and this will go out for constituent review/input and return back to another CCC meeting.
V.	BP 2330 – Quorum and Voting	Ed	2 minutes	There was some discussion about the CA Constitution reference. Mark will work on a revision and bring back to another CCC meeting.
VI.	BP 2720 – Communications Among Board Members	Ed	2 minutes	There was some discussion about the Government Code Reference. Mark will revise and bring back to another CCC meeting.
VII.	BP 3900 – Speech: Time, Place and Manner	Ed	2 minutes	There was some discussion about the Ed Code reference and the wording of

				the BP. Mark will review and revise and bring back to another CCC meeting.
VIII.	BP & AP 4100 – Graduation Requirements for Degrees and Certificates	Ed	2 minutes	There was some discussion about the Bachelor Degree Program and including the language into the BP/AP. It was agreed to revise and bring back to another CCC meeting.
IX.	AP 4222 – Remedial Coursework	Ed	2 minutes	There was some discussion about AB705 and the effects of the language in the AP. It was agreed to revise and bring back to another CCC meeting.
FUTURE A	AGENDA ITEMS:			
NEXT N	MEETING DATE:			
Februa	ry 27, 2019			

AP 3720 Computer, Network and Telecommunications Use

References:

17 U.S.C. Section 101 et seq.;
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1(b);
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

The District Computer, Network and Telecommunications systems, and the data that resides upon them, are the sole property of Antelope Valley Community College District; except where explicitly addressed by collective bargaining agreements. The Computer, Network and Telecommunications systems are for District instructional and work related purposes only.

This procedure applies to all District students, faculty, and to others granted use of District information resources. A user is defined as any individual or group who uses college technology or computing facilities resources.

This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and telecommunication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, personal computers, personal digital assistants (PDAs)mobile devices, handheld computing or telecommunications devices, workstations, mainframes, minicomputers, and associated peripherals, software, networks, telephone and telecommunications equipment, including cellular telephones, and information resources, regardless of whether used for administration, research, teaching or other purposes.

AVC Information Technology Resource Guidelines

The District shall produce and maintain guidelines that clarify procedures or processes relating to the use of District information technologies. These guidelines shall be reviewed regularly for relevance and made available to the public.

Conditions of Use

Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Account Provisioning and Deprovisioning

All employees and students are assigned an email account upon joining the college. Email is the official channel for all communications from the college. All employees and students are encouraged to check it regularly to stay current on all issues related

to instruction and services. Upon departure from the college, all students, retirees, and emeriti may retain their email account. Employee access that does not meet the above criteria may be deprovisioned upon separation. Access to services within myAVC will be deprovisioned two-years after departure. Accounts for persons no longer actively affiliated with the District will be disabled after one year of inactivity. If you need access to records that are within myAVC, please contact the appropriate office directly.

Legal Process

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Copyrights and Licenses

Computer user<u>User</u>s must respect copyrights and licenses to software and other on-line information.

Copying

Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users

The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased by the District, unless otherwise stipulated in the purchase contract.

Copyrights

In addition to software, all other copyrighted information (text, images, icons, programs, audio, video, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited. Refer to the AVC Computer Use and Electronic Mail Guidelines for additional information.

Integrity of Information Resources

Computer user Users must respect the integrity of computer-based information resources.

Modification or Removal of Equipment

Computer and telecommunications users must not attempt to modify or remove computer, network or telecommunications equipment, software, or peripherals that are allocated to other District users without proper authorization.

Unauthorized Use

Users must not interfere with others' access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be availablethat adversely impact performance of the network; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

Unauthorized Programs

Users must not intentionally develop or use programs which disrupt other computer userusers or which access private or restricted portions of the system, or which damage the software or

hardware components of the system. Computer userUsers must ensure that they do not use programs or utilities that interfere with other computer userusers or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and procedure and may further lead to civil or criminal legal proceedings.

Unauthorized Access

Computer user User's must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Abuse of Computing Privileges

Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

Reporting Problems

Any defects discovered in system accounting or system security must be reported promptly to the appropriate administrator so that steps can be taken to investigate and solve the problem.

Password Protection

A <u>computer useruser</u> who has been authorized <u>to use afor</u> password-protected accounts may be subject to both civil and criminal liability if the user discloses the <u>ir</u> password or otherwise makes the account available to others.

Usage

Computer user Users must respect the rights of other-computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may be subject to civil or criminal lability violate applicable law.

Unlawful Messages

Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, <u>malicious</u>, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

Commercial Use

Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions. District information resources may not be used for commercial purposes. Users are also reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use. However, where legally permissible, District electronic media such as message boards or mail systems may be designated for selling or fundraising.

Information Belonging to Others Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, voice messages or passwords belonging to other users, without the permission of those other users. [RS1]

Rights of Individuals

Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.

User identification

Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

Political, Personal and Commercial Use

The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters. Use of District resources for personal gain is expressly prohibited.

Political Use

District information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws.

Personal Use

District information resources should not be used for personal activities not related to appropriate District functions, except in a purely incidental manner.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of Antelope Valley Community College District network, telecommunications and computer resources which discriminates against any person in violation of Board Policy 3410. No user shall use the District network, telecommunications or computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy

The District reserves the right to monitor all use of the District network and computer resources to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure

Users must be aware of the possibility of unintended disclosure of communications.

Retrieval

It is often possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

Public Records

The California Public Records Act (Government Code Sections 6250 *et seq.*) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network and computer must be disclosed if requested by a member of the public, in accordance with BP 3300 & AP3300.

Litigation

Computer transmissions and electronically stored information may be discoverable in litigation.

Dissemination and User Acknowledgment

All users shall be provided access to these procedures and be directed to familiarize themselves with them. Periodically users will be reminded of these procedures.

Users shall acknowledge that they have reviewed BP 3720 and the associated procedures and guidelines in the manner and frequency as specified in the IT Resource Guidelines. This acknowledgement is a condition of use of any District information technology resource.

Revised: 11/7/05, 1/8/07, 9/10/07

AP 3721 <u>Virtual Private</u> Network <u>(VPN)</u> Remote Access Procedure

Reference:

An expansion of mobile employees, and the need for after hours and remote access by employees and partners necessitates procedures for such. Secure/encrypted access to college resources is essential for off campus, after hours, or vendor sponsored access. Permission to use the college's Virtual Private Network (VPN) is subject to the approval of the Executive Director, Technology, and is allowed only under the following circumstances:

Vendor Support of Network Services

The district relies on vVendor support to assist with the administration of for select network computing or network resources systems to facilitate. Several departments have requested the ability to allow vendors and consultants to remotely connect to the district network in order to fix an urgent issueaccess, or to help keep-reduce consultant fees to a minimum by reducing the need for travel expenses, or and in accommodation fors when services could be rendered from a distance. Previously, AVC did not have the technology to allow vendors to connect to the district network without exposing the network to unnecessary risks. Requests are to be submitted for review to help@avc.edu. Vendor VPN access will have a CMS or Administrative sponsor, will have a ninety (90) day expiration, and can be renewed by email request by the sponsor by email or support ticket.

Employee Remote Access

To ensure secure access of resources from outside the college network, employees will be granted VPN access for portable devices. Use of the VPN is expressly for access of college resources during in execution of the employee's duties. After hours use of VPN services for employees is still subject to Policy, Practices, and CBA conditions for overtime, and is subject to advanced approval of supervisors. Such accounts will have a one hundred eighty (180) day expiration date, and can be renewed by request of their supervisor by email or help desk ticket.

Access Requirements

Remote access to the district network resources is for contractors and vendor support personnel only, in accordance with application maintenance agreements or a well defined business need, must meet certain criteria. —To defend the district network from malware and other potential threats to network and data security, vendors, and contractors, and employees will must meet certain security criteria before they will be allowed to connect to the network remotely use industry accepted best practices to ensure systems are safe and secure. Contractor and vendor www. Workstations must be current with operating system and application security patches and have anti-virus software loaded and up to date. before a connection with the AVC network will be established. Devices may be subject to interrogation by a remote security tool to ensure compliance. Failure to meet compliance will result in suspension of access.

Remediation (For Vendors and Contractors)

If remote connection to the AVC network is denied because of insufficient security software, the contractor or vendor simply has to devices will need to be brought update or install the missing components current (e.g., anti-virus or operating system patches) and attempt a

reconnection to the district remote access device. Contact the help desk and account will be reactivated for purposes of examination. The software on the remote access device (VPN client) will ensure that the workstation the contractor or vendor or employee is connecting from has met AVC network security requirements. If all workstation prerequisites have been met, the software will establish the connection.

4/13/09

Revised: 01/07/2019 (anticipated adoption)

AP 3722 Acceptable Use Agreement

Reference:

Antelope Valley College (AVC) provides access to its computing, communications and information technology resources in-to. These resources are the property of AVC and support of the delivery of the college's academic mission and community and accordingly, t. These resources (the equipment and content) are the property of AVC, and hey should be used responsibly. These resources include: the physical data and wireless communications network; and all college computers, printers, scanners and other hardware equipment attached to that network, as well as all portable hardware, system software, telephone systems, and means of access to the Internet.

All employees, students, or eampus-visitor, are subject to the provisions of this policy, and services shall abide by this policy, and all applicable local, state, and federal statutes. With regard to the Use of any computing, communications and information-technology resources of Antelope Valley College, explicitly affirms acceptance of all users understand and agree to the following provisions the following conditions of use:

- The district's computing, communication and information technology resources are provided for the support of its educational and service goals. and Tthe use of such resources for any other purposes is prohibited.
- Users may not use district resources for conducting a private business or for personal financial gain, or partisan political activities.
- However, ilncidental personal use is permissible permitted so-as long as: (a) it does not violate state or federal law or AVC policy, (b) it does not consumes only-more than a trivial amount of system-resources or time, (c) and, it does not interfere with productivity of students or district employees the college, it's employees, students, or visitors., and (d) it does not preempt any district activity. All users of district information technology resources and services shall abide by this policy along with any local, state, and federal law that may apply.
- All users are subject to both the provisions of this policy, as well as any policies specific to the individual systems they use.
- To protect ensure, and safeguard, the integrity of computing resources, passwords, access codes, or account names account names and passwords must not be shared-with others. Additionally, pPasswords will be subject to complexity requirements and users will be required to change their passwords periodically.—These specifications will be reviewed and published annually by the Information Technology Committee.
- Most educational materials (both commercial and district employee created, including software) are protected under copyright. Any violation of the rights of a person or entity protected by copyright law is prohibited. The unauthorized duplication, installation, or distribution of copyrighted computer software or content utilizing the district's computing, communications and information resources is is specifically expressly prohibited. Unauthorized software, installed on district owned computerstechnology, will not be supported and may be removed if deemed necessary in volition of copyright or district policy.
- Users may not <u>bypass</u>, <u>utilize any connect any system/equipment or install</u>
 software <u>device or which software</u>, <u>which circumvents authenticated protections to could</u>

allow any user to gains access to the district's systems or services, and information without coordinating with Information Technology Services (ITS).

- Users may not use district resources for conducting a private business or for personal financial gain.
- Intentionally sending or accessing pornography or patently obscene material other than
 for authorized research or instructional purposes is prohibited. The definition of
 "pornography" and "obscene" shall be as determined by law.
- Computer and information technology uusers should consider be mindful of the inherently open nature of information transferred electronically, and should not assume an absolute degree of privacy or of authenticated restricted access to such information. The district provides the highest degree of security possible when transferring and hosting data, but disclaims responsibility if these security measures are circumvented and the information is compromised.
- The district is not responsible for loss of data, time delay, system performance, software performance, or any other damages arising from the use of district computing resources.
- Authorized district personnel may, while performing routine or investigative operations have access to data, including electronic mail, web browser information, and any other personal data stored on district computers.
- Except where explicitly addressed by labor agreements RS11, a-All content of stored on district technology is deemed to be the property of the district, including that generated by incidental use.
- Student workstations are subject to routine monitoring. Computer screens attached to student workstations, particularly those accessing the Internet, may be periodically viewed by district personnel to monitor compliance with district policy. However, t
- The district shall not routinely or arbitrarily monitor incidental personal use of district resources by employees. Neither the district nor any employee shall disclose the contents of any observed personal data to any other person or entity except as required by law or Board Policy.
- Activities that place excessive strain on network resources should be avoided.
 Conducting activities such as Peer to peer (P2P) file sharing or use of any other similar technologies is prohibited and subject to disciplinary action.
- The confidentiality of student and employee information is protected under federal and state law and/or regulations. Any information regarding students or employees that might be accessed in the course of using an AVC computer may only be shared with those who are authorized to have such information. Employees and students may not change, alter, copy, or divulge any such information unless it is required to carry out an assignment. Access to, or alteration of, such information is expressly limited to execution of day-to-day assigned duties.
- Employees and students should ensure that their workstation is logged off, or shutdown, -before stepping away from the computer.

Users found in violation of the district's computer and information technology use policies, are subject to disciplinary action, as described in the enforcement section of this document below.

Selected Examples of Unacceptable Use:

- Revealing/Sharing <u>user-id or passwords to with others</u>, <u>or using someone else's account, or allowing someone else to use of your account <u>by others</u>.
 </u>
- <u>Attempting to defeat data protection schemes or altering network configurations to uncover security vulnerabilities.</u>
- Using someone else's account. Utilizing network or system id numbers/names that are not assigned for one's specific use on the designated system.
- Attempting to authorize, delete, or alter files or systems not created by oneself without proper authorization as described in the Computer Use and Electronic Mail Guidelines.
- Not complying with requests from AVC personnel to discontinue activities that threaten degrade or interrupt the integrity or stability of computing resources.
- Attempting to defeat data protection schemes or to uncover security vulnerabilities.
- Connecting unauthorized <u>personal equipment</u> <u>wireless access points and other computer equipment</u> to the campus <u>physical</u> network without <u>coordinating authorization from with ITS.</u> (<u>Devices such as PDAs, printers, and USB drives that connect to a computer and not directly to the network are acceptable.</u>)
- Registering an Antelope Valley College IP address with any other domain name.
- Unauthorized network scanning or attempts to intercept network traffic.
- Malicious disruptions such as , e.g., introducing a computer virus or malware to the campus network, or -
- Hharassing or threatening other users of the campus network.
- Using district resources for partisan political activities where prohibited by federal, state or other applicable laws.

To ensure the integrity and reliability of <u>computer and communications</u> <u>technologyall</u> resources, <u>all</u> users are encouraged to repo<u>rrt</u> improper use and violations of this agreement <u>Individuals may report suspected violations of this agreement</u> to an AVC faculty member, supervisor or administrator as appropriate.

Enforcement1

Individuals may report suspected violations of these guidelines to an AVC supervisor, faculty member or administrator as appropriate. Reports of violations that are received by ITS will be forwarded to the appropriate supervisor or administrator.

- Disciplinary action maywill be taken in accordance with AVC applicable policies, collective bargaining agreements, state or federal statutes.
- Minor infractions of these guidelines, or those that appear accidental in nature, are
 typically handled internally by the appropriate supervisor or administrator, in consultation
 with ITSthe Executive Director, Technology. In some situations it may be necessary to
 suspend account or computer access to prevent ongoing misuse.
- More serious infractions or repeated minor violations may result in the temporary or permanent loss of access.

¹ This section is taken directly from the Computer Use and Electronic Mail Guidelines document AP 3720: Computer, Network, and Telecommunications Use.

- Offenses that are clearly in violation of local, state or federal laws will be reported to the
 Los Angeles County Sherrif's Department and -result in the immediate loss of access to
 computing resources and maybe subject to disciplinary suspension or termination from
 employment or expulsion; and/or civil or criminal legal action.
- Disciplinary action may be taken in accordance with one or more of the following: AVC policies, California law or the laws of the United States.

Minor infractions of these guidelines or those that appear accidental in nature are typically handled internally by the appropriate supervisor or administrator, in consultation with ITS. In some situations it may be necessary, however, to suspend account or computer access to prevent ongoing misuse while the situation is under investigation.

More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of college policies or repeated violations of minor infractions may result in the temporary or permanent loss of access to computing facilities.

Offenses that are clearly in violation of local, state or federal laws will result in the immediate loss of access to computing resources and will be reported to the appropriate law enforcement authorities. In addition, disciplinary action, up to and including dismissal, may be applicable under other AVC policies, guidelines or collective bargaining agreements.

10/11/10

Revised: $\frac{9601}{9807}$ (anticipated adoption)

AP 6200 Budget Preparation

References:

Education Code Section 70902(b)(5); Title 5 Sections 58300 et seq; ACCJC Accreditation Standard III.D

- The budget process will include consultation with appropriate groups and will link resource allocations to institutional planning.
- The District will have a goal to maintain a 12% reserve in any current budget year to pay obligations, or 60 days of cash on hand in the unrestricted fund, whichever is greater.
- A budget calendar that includes presentation of the tentative and final budgets will be distributed with the annual budget call. The tentative budget shall be presented no later than July 1 [Title 5 Section 58305(a)], and the final budget no later than September 15 [Title 5 Section 58305(c)]. A public hearing on the budget shall be held on or before September 15 [Title 5 Section 58301].
- Two copies of the adopted budget to be submitted to the California Community College Chancellor's Office on or before September 30 [Title 5 Section 58305(d)].
- Submission of appropriate financial reports to include upcoming budgets will be submitted to the California Community College Chancellor's Office via the CCFS311 Report.
- 1. Budget Preparation Philosophy: Refer to Chapter 3, AP 3250 Institutional Planning
- 2. Budget Development Processes: Refer to Chapter 3, AP 3250 Institutional Planning
- 3. Criteria and Guidelines for Planning and Budgeting: Refer to Chapter 3, AP 3250 Institutional Planning

4. District Budget Calendar:

The tentative District budget shall be prepared by the Vice President, Business Services, recommended by the President, approved by the Board, and filed with the Chancellor's Office by July I.

The Board shall hold a public hearing on the budget on or before the 15th of September, but not earlier than three days following availability of the budget for public inspection. Adoption of the District budget by the Board shall be accomplished on or before September 15 to allow for the filing of the adopted budget (two copies of 311 forms) with the Chancellor's Office on or before September 30.

Revised 2015 Revised 2018

BP 6250 Budget Management

Reference:

Title 5 Sections 58307, 58308.

The budget shall be managed in accordance with Title 5 and the CCC Budget and Accounting Manual. Budget revisions shall be made only in accordance with these policies and as provided by law.

The District is committed to addressing its long-term liabilities. Revenues accruing to the District in excess of amounts budgeted shall be added to the District's reserve for contingencies to a pension stabilization trust fund, so long as it can be supported in the multi-year budget projections and within the board goal of 12% reserve levels. The intent of the pension stabilization fund is to ensure that the District can meet its current and future employer-funded pension obligations. Additionally, half of all new one-time funding will be directed to the pension stabilization fund until that fund is self-supporting. Any additional revenues above expenditures shall be added to the District's reserves for contingency. They These funds are available for appropriation only upon a resolution of the Board that sets forth the need according to major budget classifications in accordance with applicable law.

Board approval is required for changes between major expenditure classifications. Transfers from the reserve for contingencies to any expenditure classification must be approved by a two-thirds vote of the members of the Board. Transfers between expenditure classifications must be approved by a majority vote of the members of the Board.

See Administrative Procedure # 6250

Adopted: 5/8/06, Revised: 12/14/15 Revised: 3/2019

BP 6975 Export Control Policy

Reference:

U.S. Export Administration Act implemented by export Administration Regulations (EAR), U.S. Arms Export Control Act implemented by International Traffic in Arms Regulations (ITAR), and U.S. Office of Foreign Asset Control Regulations (OFAC).

It is the policy of the Antelope Valley Community College District to fully comply with United States export control laws and regulations. Export controls are a complex set of federal regulations that apply to the release of certain information, commodities, technologies, and software to foreign nationals in the United States and abroad.

Although the District maintains an open academic environment in support of its teaching and research mission, the District is committed to complying with all United States export control laws in both research and non-research activities. While the majority of activities at the District are not subject to export control restrictions or licensing requirements, it is the responsibility of each member of District to be aware of the requirements and determine how export controls might apply to their activities.

This Board Policy applies to all District staff, faculty, academic appointees, students (including student employees), and non-employee participants in District programs and activities. Export control violations can impact both the District and the individuals who violate the law and can result in severe criminal and/or civil penalties for non-compliance.

See Administrative Procedures #6975
Adopted:

AP 6975 Export Control Administrative Procedure

Reference:

U.S. Export Administration Act implemented by Export Administration Regulations (EAR), U.S. Arms Export Control Act implemented by International Traffic in Arms Regulations (ITAR), and U.S. Office of Foreign Asset Control Regulations (OFAC).

I. Overview of Export Controls

Export controls are a complex set of federal laws and regulations that regulate the release of certain commodities, technologies, and software to foreign nationals in the United States and abroad. The export control regulations are intended to protect U.S. foreign policy interests, protect national security, prevent terrorism and the proliferation of weapons of mass destruction, and preserve U.S. economic competitiveness. In general, anything leaving the U.S., such as research data, other intellectual property, documents or tangible items, whether shipped, carried and transported in any way is an "export." The releasing or otherwise transferring certain technical data and/or technology to a foreign person in the U.S. is a "deemed export" subject to the export control regulations. The particulars of each activity must be analyzed to determine the applicability of export control regulations and whether any exceptions apply.

II. <u>Export Controls Laws and Regulations</u>

Export Controls exist under three primary federal laws and associated regulations that are implemented by the U.S. Department of Commerce, the U.S. Department of State and the U.S. Department of Treasury as follows.

The Export Administration Act of 1979, as amended, authorizes the Department of Commerce, in consultation with other appropriate agencies, to regulate the export or re-export of certain U.S. origin goods, software, and technology. The Export Administration Regulations ("EAR") are administered by the United States Department of Commerce Bureau of Industry and Security (15 C.F.R.§ § 730-740).¹ EAR focusses on items that can have both regular civilian uses and can have military applications, often described as "dual-use" and are identified on the Commerce Control list.² Items subject to the EAR include purely civilian items, items with both civil and military terrorism or potential weapon of mass destruction-related applications, and items that are exclusively used for military applications but that do not warrant control under the International Traffic in Arms Regulations.

¹ https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

²https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

The Arms Export Control Act ("AECA") is implemented by the Department of States International Traffic in Arms Regulations ("ITAR") (22 C.F.R. § § 120-130).³ All persons or entities that engage in the manufacture, export, or brokering of defense articles and services must be registered with the U.S. government. The ITAR sets out the requirements for licenses or other authorizations for specific exports of defense articles and services. This regulation is the most restrictive and has stringent requirements for who can perform this type of research or have access to the defense articles and services. An overview of U.S. Export Control systems is provided by the Department of States at: https://www.state.gov/strategictrade/overview/.

The U.S. Department of Treasury implements the Office of Foreign Asset Control Regulations ("OFAC") (31 C.F.R. § § 501-598). OFAC regulations mostly affect foreign collaborations, international shipments and lectures or research abroad.⁴ The OFAC administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. Additional information on the OFAC is available at the U.S. Department of Treasury Resource Center at: https://www.treasury.gov/resource-center/fags/Sanctions/Pages/ques_index.aspx

III. Activities that Generally Require Export Control Review

It is up to each individual to determine if their work may involve information or activities requiring Export Control review. The following are examples, but not an exhaustive list, of activities requiring Export Control review: export of goods (equipment, hardware, materials); export of technology (technical information and data including technology sent via email); export of software/code (including software sent via email); travel to other countries; visits by foreign nationals to District; disclosure of controlled information and materials to foreign nationals in the U.S., collaboration with foreign nationals or foreign companies.

IV. Fundamental Research Exclusion

The Fundamental Research Exclusion ("FRE") provides that technology or software that arises during, or results from, fundamental research and is intended to be published is excluded from the export control regulations. The FRE generally permits U.S. higher educational institutions to allow foreign members of their communities (e.g., students, faculty and visitors) to participate in research involving export-controlled information on campuses in the U.S. without obtaining a license. However, the FRE does not permit the transfer of export controlled materials or items abroad, even to research collaborators. The FRE does not apply to research with restriction on publication of the results of the project.⁵ Fundamental Research is defined under EAR to mean:

³ https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

⁴ https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

⁵ See 22 C.F.R. § 120.11(a)(8); 15 C.F.R. § 734.8(c); and 10 C.F.R. § 810.3.

Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons. (15 C.F.R. § 734.8(c)).

Fundamental Research is defined in ITAR to mean:

(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if: (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable. (22 C.F.R. § 120.11(a)(8)).

V. <u>District Export Compliance Officer</u>

The District's Export Compliance Officer (ECO) in the office of the Executive Director of Business Services in conjunction with Purchasing and Contracts is available to assist members of the District to assess their export control obligations and facilitates the procurement of export licenses when required.

- A. The District's ECO implements District practices and procedures involving:
 - 1. Identification, review and determination of any export control requirements, including control plans and licensing exceptions that may apply;
 - 2. Identification of license exceptions or exclusions;
 - 3. Submit export license application when an export license is required;
 - 4. Conduct screening for restricted individuals and entities;
 - 5. Document and communicate export control decisions;
 - 6. Monitor export controlled projects for regulatory compliance;
 - 7. Establishment of Technology Control Plans when required;
 - 8. Establish procedures for individuals to report potential non-compliance;

- 9. Review and investigate reports of non-compliance;
- 10. Develop and implement export controls training program for the District;
- 11. Develop procedures for obtaining approval of foreign travel, for hosting foreign guests and for international collaborations;
- 12. Develop and implement international shipping and purchasing practices for export controls compliance.

B. Compliance Assistance for District Employees

District employees are responsible for identifying whether their activities may involve export control issues and for contacting the ECO for assistance in compliance with applicable laws and regulations. Compliance with export control regulations requires the cooperation and shared responsibility of many offices and persons across the District. The ECO shall be the District's point of contact in charge of the District's export control training and compliance efforts.

C. Record-Keeping

U.S. export control regulations (e.g., EAR, OFAC, ITAR) contain specific recordkeeping requirements that must be satisfied. The District must keep copies of all export documentation as required by the controlling regulations, and consistent with District document retention policies. In the event of a conflict between the retention periods in the applicable U.S. export regulations and the District document retention policy, the periods specified in the federal regulations shall take precedence.

D. Potential Violations

The District will respond promptly to all reports of non-compliance and will take appropriate action to correct and prevent future violations. The District's ECO shall investigate all reports of suspected violations and coordinate with legal counsel and other District leadership as necessary.

E. Disclosure to Federal Agencies

Federal regulations may require reporting of any violations to the cognizant agency responsible for the export control regulation and to federal sponsors. Voluntary and timely self-disclosures may mitigate the seriousness of a penalty. The ECO shall coordinate with the District's leadership and legal counsel concerning advance notification to the relevant governmental entity.

ᄱ	lop:	tad	١.
٦u	w	LEU	١.

AP 4230 Grading and Academic Record Symbols

Reference:

Title 5, Section 55023 and 55024

Evaluative symbols:

```
A - Excellent (Grade Point = 4)
```

B - Good (Grade Point = 3)

C - Satisfactory (Grade Point = 2)

D - Less than satisfactory) (Grade Point = 1)

F - Failing (Grade Point = 0)

P - Passing (At least satisfactory - Units awarded not counted in GPA)

NP - No Pass (Less than satisfactory), or failing - units not counted in GPA)

SP – Satisfactory Progress towards completion of the course (Used for noncredit courses only and is not supplanted by any other symbol)

Non-Evaluative symbols:

I -Incomplete

IP - In progress

RD - Report delayed

W - Withdrawal

MW - Military Withdrawal

EW - Excused Withdrawal

Final grades are issued at the end of each semester.

Grades are calculated on a 4.0 scale. (A=4 pts; B=3pts; C=2 pts; D= 1 pt; and F=0 pts)

Grades of P, NP, I, IP, RD, and W have no points attached and are not used in calculating grade point average.

Students' grades in each course will be recorded on their transcripts at the end of each semester.

I (Incomplete) – Used to indicate incomplete academic work for unforeseeable, emergency, and justifiable reasons at the end of the term.

An incomplete contract must be completed and the terms and conditions agreed upon by both the student and faculty. The condition for removal of the "I" and the grade to be assigned in lieu of its removal shall be stated by the instructor in the contract which will be held on file in the Admissions Office.

A student has 1 year to complete the obligations of the incomplete contract. This record

shall remain on file until the "I" is made up or the time limit has passed. A final grade shall be assigned when the work stipulated has been completed and evaluated or when the time limit for completing the work has passed.

If the terms and conditions of the contract are not fulfilled the "I" will convert to a grade of "F." A student may petition for an extension of time due to unusual circumstances before the time limit has passed. The "I" symbol shall not be used in calculating units to determine grade point average.

IP (In Progress) – Used to denote that the class extends beyond the normal end of an academic term. It shall indicate that work is "in progress," but that assignment of a substantive grade must await its completion. The "IP" symbol shall remain on the student's permanent record in order to satisfy enrollment documentation. The appropriate evaluative grade and unit credit shall be assigned and appear on the student's record for the term in which the course is completed. The "IP" shall not be used in calculating grade point average. If a student enrolled in an "open-entry, open-exit" course is assigned an "IP" and does not re-enroll in that course during the subsequent term, the appropriate faculty will assign an evaluation symbol (grade) to be recorded on the student's permanent record for the course.

RD (**Report Delayed**) – Used when there is a delay in reporting the grade of a student due to circumstances beyond the control of the student. It is a temporary notation to be replaced by a permanent symbol as soon as possible. "RD" shall not be used in calculating grade point average.

W (Withdrawal) - Used to denote withdrawal from a class or classes through the last day of the fourteenth week of instruction. The academic record of a student who remains in class beyond the fourteenth week will be graded for the course. For a "W" grade, no notation shall be made on the academic record of a student who withdraws during the first four weeks of a semester. The "W" shall not be used in calculating grade point average, but excessive "W's" shall be used as a factor in academic probation and dismissal procedures (See BP and AP 4250).

A student planning to withdraw from one or more classes may do so online or in person through the Office of Admissions & Records by submitting a withdrawal form. Failure to do so will result in the student's being awarded a final grade at the discretion of the instructor for each class in which the student is registered.

MW-_(Military Withdrawal): The "MW" symbol may be used to denote military withdrawal of an active or reserve member of United States Military in accordance with Title 5 Section 55024._

EW - Excused Withdrawal: The "EW" symbol may be used to denote withdrawal in accordance with Title 5 Section 55024. The "EW" occurs when a student is permitted to withdraw from a course(s) due to specific events beyond the control of the student affecting his or her ability to complete a course(s) and may include a job transfer outside the geographical region, an illness in the family where the student is the primary caregiver, when the student who is incarcerated in a California state prison or county jail is released from custody or involuntarily transferred before the end of the term, when the student is the subject of an immigration action, or other extenuating circumstances as described in 55024.

2/6/06 3/10/08

Revised: 10/9/17

Revised: summer 2018

AP 5010 Admissions

Reference:

Education Code 76000; 34 Code of Federal Regulations Section 668.16(p) (U.S. Department of Education regulations on the Integrity of Federal Student Financial Aid Programs under Title IV of the Higher Education Act of 1965, as amended); ACCJC Accreditation Standard II.C.6

Designated authority and responsibility for the following admissions processes resides with the Dean of Student Services (Admissions & Records) Enrollment Services.

- Admission procedures for students over 18 with a high school diploma and admission of any California resident under 18 years of age possessing a high school diploma or the equivalent thereof.
- Admission criteria and procedures for students over 18 without a high school diploma and admission of any California resident 18 years of age or older without a high school diploma
- who can benefit from education,
- Admission procedures for non-resident students including a determination of residency status (AP 5015).
- Publication of admissions policies and procedures in the college catalog, schedule of classes, and the college Website.
- Concurrent enrollment of high school and other young students including special full time and part time students (AP 5011).
- Admission of all 16 and 17 year olds who have not completed high school and are eligible to be
 admitted by examination. Students successfully completing such examination will be awarded
 a "Certificate of Proficiency" by the State Board of Education that authorizes the student to
 enroll at Antelope Valley College with regular student status.

The Vice President of Academic Affairs shall be responsible for evaluating the validity of a student's high school completion if the college or the United States Department of Education has reason to believe that the high school diploma is not valid or was not obtained from an entity that provides secondary school education.

2/6/06

Revised 10/18

AP 5012 International Students

Reference:

Education Code Sections 76141; 76142; Title 5, Section 54045; Title 8, U.S.C. Section 1101. et seq.

International Student Admission Requirements and Procedures

The International Student application process includes submission of appropriate visa information from the country of residence, including INS forms, application for admission, student information form, high school diploma, official high school transcripts with notarized English translation, original letter of reference on letterhead, birth certificate or valid passport with recent photograph, notarized affidavit of financial support, notarized affidavit of sponsor, notarized affidavit of sponsor for free room and board, copy of deed lease agreement or rental agreement of property, and a medical insurance policy in English.

Students who will be attending pursuant to an F-1 visa, must submit all of the same paperwork required for the International Student application process stated above in order to substantiate issuance by the District of form I-20.

International Students must have a TOEFL (Test of English as a Foreign Language) score (minimum 133 on computer-based test or 450 if paper test), if applicable. Other assessments may satisfy this requirement such as

-<u>iIELTS (The International English Language Testing System) with a score of 5.0 or s</u>Satisfactory SAT/-or ACT-scores may be used to satisfy this requirement. Other assessments results must be equal to or greater than the TOEFL or iLELTS requirement.

Residence determination includes review of whether student holds a visa that requires the student to have a residence outside of the U.S., or entered the U.S. under a visa that permits entry solely for a temporary purpose.

International Students are eligible for exemptions from nonresident tuition as authorized by Education Code Section 76140(a)(2) for financial need.

Nonresident tuition fees applicable to non-citizens who have not or cannot establish residence are determined by calculating an amount not to exceed the amount expended by the District for capital outlay in the preceding fiscal year divided by the total full-time equivalent students. This fee cannot exceed 50 percent of the nonresident tuition charged other nonresidents.

2/6/06

Revised 11/18

AP 5031 Instructional Materials Fees

Reference:

Education Code Section 76365; Title 5 Section 59400 et seg.

Students may be required to provide instructional and other materials required for a credit or noncredit course. Such materials shall be of continuing value to a student outside of the classroom setting and shall not be solely or exclusively available from the District.

Required instructional materials shall not include materials used or designed primarily for administrative purposes, class management, course management, or supervision.

Where instructional materials are available to a student temporarily through a license or access fee, the student shall be provided options at the time of purchase to maintain full access to the instructional materials for varying periods of time ranging from the length of the class up to at least two years. The terms of the license or access fee shall be provided to the student in a clear and understandable manner prior to purchase.

<u>Instructors shall take reasonable steps to minimize the cost and ensure the necessity of instructional</u> materials.

The District will publish these regulations in each college catalog.

Definitions

"<u>Required il</u>nstructional and other materials" means any tangible personal property which is owned or primarily controlled by an individual student.

"Tangible personal property" includes electronic data that the student may access during the class and store for personal use after the class in a manner comparable to the use available during the class.

"Required instructional and other materials" means any instructional and other materials which a student must procure or possess as a condition of registration, enrollment or entry into a class; or any such material which that the instructor determines is necessary to achieve these required objectives of a course which are to be accomplished under the supervision of an instructor during class hours.

"Solely or exclusively available from the District" means that the <u>instructional</u> material is not available except through the District, or that the District requires that the <u>instructional</u> material be purchased or procured from it. A material shall not be considered to be solely or exclusively available from the District if it is provided to the student at the District's actual cost; and 1) The <u>instructional</u> material is otherwise generally available, but is provided solely or exclusively by the District for health and safety reasons; or 2) The <u>instructional</u> material is provided in lieu of other generally available but more expensive material which would otherwise be required.

"Required instructional and other materials which are of continuing value outside of the classroom setting" are materials which can be taken from the classroom setting and which are not wholly consumed, used up, or rendered valueless as they are applied in achieving the required objectives of a course to be accomplished under the supervision of an instructor during the class hours.

Establishing Required Materials and Related Fees

Determination of Fees:

Division deans and discipline faculty will determine costs through a comparative approach that seeks

to obtain material at the lowest cost possible without compromising quality. Whether a materials fee meets the criteria and are appropriate for a course will be determined by the Academic Policies and Procedures Committee. New or revised materials fees must be approved by the Academic Policies and Procedures Committee and the Board of Trustees.

Materials will be provided by faculty during course or lab sections.

Announcement of Fees

Course material fees shall be printed in the semester schedule. Courses with fees will be properly flagged on records used in the Admissions Office. A fee policy and regulations will be included in the College Catalog.

Collection of Fees

Course material fees will be collected at the time of registration and after courses have been selected by students. Registration in courses will be provisional until the cashier has received full payment. Checks returned by a student's bank for any reason will result in a suspension of enrollment until valid payment has been received.

Refund of Fees

Material fees will be refunded on a prorated basis. Requests for refunds must be in writing accompanied by a drop slip signed by the instructor with the prorated amount of material fee to be refunded. Fees collected for classes cancelled by the District will be refunded.

Allocation and Disbursement of Material Fees

Each term, material fees collected and deposited will be allocated to the respective line item budgets. Disbursement of the material fees will be based on purchasing guidelines.

Business Services is responsible for gathering related data and responding to the State Chancellor's Office inquiries regarding these fees.

4/14/08

Revised 11/2018

BP 2330 Quorum and Voting

Reference:

Education Code Sections 72000(d)(3, 81310 et seq., 81365, 81511, 81432; Government Code Section 53094; Code of Civil Procedure Section 1245.240; California Constitution Article XIII A, Section 1, Subdivision (b), paragraph (3), and Article XVI, Section 18, Subdivision (b).

A quorum of the Board shall consist of a simple majority, (3) members.

The Board shall act by majority vote of all of the membership of the Board, except as noted below.

No action shall be taken by secret ballot.

The following actions require a two-thirds majority of all members of the Board:

- Resolution of intention to sell or lease real property (except where a unanimous vote is required);
- Resolution of intention to dedicate or convey an easement;
- Resolution authorizing and directing the execution and delivery of a deed;
- Action to declare the District exempt from the approval requirements of a planning commission or other local land use body;
- Appropriation of funds from an undistributed reserve;
- Resolution to condemn real property;
- Resolution to pursue the authorization and issuance of bonds.

The following actions require a unanimous vote of all members of the Board:

- Resolution authorizing a sale or lease of District real property to the state, any county, city, or to any other school or community college district;
- Resolution authorizing lease of District property under a lease for the production of gas.

Adopted: 7/5/05 Reviewed: 8/8/16

Revised: 3/11/19

BP 2720 Communications among Board Members

Reference:

Government Code Section 54952.2 b

Members of the Board shall not communicate among themselves by the use of any form of communication (e.g., personal intermediaries, e-mail, or other technological device) in order to reach a collective concurrence regarding any item that is within the subject matter jurisdiction of the Board. In addition, no other person shall make serial communications to Board members.

A majority of the members of the Governing Board shall not, outside a regularly scheduled meeting, use a series of communications of any kind, directly or through intermediaries, to discuss, deliberate, or take action on any item of business that is within the subject matter jurisdiction of the Board.

This policy shall not be construed as preventing an employee or official of the District from engaging in separate conversations or communications with members of the Board outside of a meeting in order to answer questions or provide information regarding a matter that is within the subject matter jurisdiction of Board, if that person does not communicate to members of the Board the comments or position of any other member or members of the Board.

Adopted: 7/5/05 Revised: 10/11/10 Reviewed: 10/10/16 Revised: 3/11/19

BP 3900 Speech: Time, Place and Manner

References:

Education Code Sections 76120 and 66301(d),(e)

Students, employees, and members of the public shall be free to exercise their rights of free expression, subject to the requirements of this policy.

The college of the District is open to the public. However, the college is a non-public forum and designated public forums available for the exercise of expression by students, employees, and members of the public are-subject to limits by the District and must be reserved.

The Superintendent/President shall enact such administrative procedures, as are necessary to reasonably regulate the time, place and manner of the exercise of free expression in the designated public forums.

The administrative procedures promulgated by the Superintendent/President shall not prohibit the right of students to exercise free expression, including but not limited to the use of bulletin boards; the distribution of printed materials or petitions in those parts of the college designated as areas generally available to students and the community; and, the wearing of buttons, badges, or other insignia. When that speech is defamatory, obscene, libelous or slanderous according to current legal standards, or which incites others as to create a clear and present danger of the commission of unlawful acts on district property or the violation of district policies or procedures, or the substantial disruption of the orderly operation of the District, the District can prohibit these forms of speech, as it may violate this section. (Educational Code 76120)

Nothing in this policy shall prohibit the regulation of hate violence directed at students in a manner that denies their full participation in the educational process (Education Code Section 66301(e)), so long as the regulation conforms to the requirements of the First Amendment to the United States Constitution, and of Section 2 of Article 1 of the California Constitution. Students may be disciplined for harassment, threats, or intimidation unless such speech is constitutionally protected. 66301(d)

See Administrative Procedure #3900

Adopted: 2/6/06 Revised: 9/10/07 Revised: 5/14/12 Revised: 3/13/17 Reviewed: 2/11/19