FOOTHILL-DE ANZA
Community College District

Chancellor's Advisory Council

Meeting Agenda – May 26, 2023, 9:00-10:30 a.m.

District Office Building (D700), Board Conference Room 101

Zoom: *https://fhda-edu.zoom.us/j/83559840180?pwd=b2JYYmRzRjluczJaMTZvTWU1VGsrUT09*

AGENDA TOPIC	PURPOSE/DESIRED OUTCOME	DISCUSSION LEADER
1. Welcome and introductions	*I* – Allow council members and guests to identify each other by name and constituent group represented and/or role at the colleges/district.	Judy Miner
2. Approval of April 28, 2023 meeting summary	*A* – Provide accurate record of previous meetings.	Judy Miner
3. Please review the drafts of the following Board Policies and Administrative Procedures: • Review New Draft BP 6450 Wireless or Cellular Telephone Use (First Reading) • Review New Draft AP 6450 Wireless or Cellular Telephone Use (First Reading) • Review Revised BP 3250 (to be revised to BP 3720 "Computer and Network Use") (Second Reading) • Review Revised AP 3250 (to be revised to AP 3720 "Computer and Network Use") (Second Reading) • Review Revised Draft BP 5030 Fees (Second Reading) • Review Revised Draft AP 5030 Fees (Second Reading)	I – Review of policy and procedures approved by the Chancellor's Cabinet for dissemination to constituents. *(Note: Pursuant to administrative procedure 2410, administrative procedures that do not involve academic and professional matters are effective upon approval of the Chancellor's Advisory Council. Board polices are not effective until approved by the Board of Trustees.)* D/A – Hear any feedback from constituency groups and approve. *(Note: Pursuant to administrative procedure 2410, administrative procedures that do not involve academic and professional matters are effective upon approval of the Chancellor's Advisory Council. Board polices are not effective until approved by the Board of Trustees.)*	Judy Miner
4. Enrollment management (standing item)	*I/D* – Gain understanding of enrollment initiatives, provide feedback/advice, and share information with constituencies.	Kris Whalen Lloyd Holmes
5. Accreditation items – Review the strategic plan document • District Strategic Plan 2024-2031 (First Reading)	I/D – David Ulate will share the draft District Strategic Plan 2024-2031 with the Chancellor's Advisory Council during the meeting.	David Ulate
6. District Governance Committee/Constituent Group Reports • Affordable Housing Task Force • District Budget Advisory Committee https://www.fhda.edu/_about-us/_participatorygovernance/B-district-budget-advisory-committee.html • Energy and Sustainability Advisory Committee https://www.fhda.edu/_about-us/_participatorygovernance/E-Energy-and-Sustainability-Advisory-Committee.html • Police Chief's Advisory Committee https://www.fhda.edu/_about-us/_participatorygovernance/G-Police-Chiefs-Advisory-Committee.html • Human Resources Advisory Committee/District Diversity and Equity Advisory Committee https://www.fhda.edu/_about-us/_participatorygovernance/F-hrac.html	*I* – Broaden awareness. Provide information for council members to disseminate to constituents about work/actions of districtwide governance groups and constituent groups.	All

RECOMMENDED EDITS

Computer and Network Use~~: Rights and Responsibilities~~

BP ~~3250~~ 3720

The Foothill - De Anza Community College District ("District") owns, **leases**, and**/or** operates a variety of computer and communication systems, including **but not limited to**, voicemail, electronic mail (e-mail), telephone, **cloud-based applications**, and access to the Internet, which are provided for the use of District faculty, administrators, staff, and students in support of the programs of the Colleges and District. Hereinafter, this system and all its component parts shall be referred to as the "District Network." This network establishes a communications platform that often substitutes for in-person meetings regarding District business.

Employees, students, or other individuals who use District computers and networks, including the information they contain and related resources, have a responsibility not to abuse those resources and to respect the rights of others. The Chancellor shall establish procedures that provide guidelines for the appropriate use of the District Network, computing equipment, and information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

~~The Computer and Network Use: Rights and Responsibilities Policy ("the Policy") applies to all members of the District community using the District Network including faculty, administrators, staff, students, independent contractors, and authorized guests. The Policy covers use of computer equipment and communication systems at any District facility in computer labs, classrooms, offices, libraries and the use of the District servers and networks from any location. If any provision of this policy is found to be legally invalid it shall not affect other provisions of the policy as long as they can be effective without the invalid provision.~~

~~**Ownership Rights**~~

~~The Policy is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, and all hardware and software components within it, is the sole property of the District which sets the terms and conditions of its use consistent with the law. Except as provided in Board Policy or collective bargaining agreements pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the District Network.~~

~~**Privacy Interests**~~

~~The District recognizes the privacy interests of faculty and staff and their rights to freedom of speech, participatory governance and academic freedom as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users anticipate. In the District Network can be subject to authorized and unauthorized access by both internal and external users. For these reasons, there are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the District Network is not to be relied upon as confidential or private. Nonetheless,~~

the District seeks to afford email communications privacy protections comparable to those it traditionally affords paper mail and telephone communications.

District Rights

System administrators may access user files or suspend services they manage without notice: 1) to protect the integrity of computer systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; or 4) when it reasonable to believe that violations of law or District policy or procedures have occurred. For example, system administrators, following organizational guidelines, may access or examine individual files or accounts based on suspicion that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board policy. Such data or information may also be used as grounds for appropriate personnel action.

User Rights

While the District monitors electronic usage as part of its normal network operating procedures, the District does not routinely inspect or monitor users' computer hardware or files, email, and/or telephone message system, nor disclose information created or stored in such media without the user's consent. The District shall attempt to notify users before accessing computer hardware and files or prior to suspending service. In the event that the District acts without user consent, under its District Rights specified above, the District shall do so with the least perusal of contents and the least action necessary to resolve the immediate situation. When the District accesses files without user consent, it shall notify the user as soon as possible of its access and provide the reason for its action.

User Responsibilities

The Board recognizes that computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources and observe all relevant law, regulations and contractual obligations.

For District employees, the intended uses of the District Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional activities. Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities provided that such use is within reason and provided that such usage is ordinarily on an employee's own time, is occasional, and does not interfere with or burden the District's operation.

"Unauthorized uses" include prohibited uses and any other use for a prohibited purpose, including illegal activities, messages which may constitute discrimination or harassment under state or federal law, or anything that interferes with the intended use. These types of prohibited uses and purposes are further defined in Administrative Procedure 3250.

All users of the District Network must read, understand, and comply with this Policy as well as Administrative Procedures 3250, and any additional guidelines established by the District. Such guidelines will be reviewed by the District and may become subject to Board approval as a District policy or procedure. By using any part of the District Network, users agree that they will comply with this Policy.

~~Copies of this Policy can be found in the policies section of the College Catalogues, Schedule of Classes, Student Handbooks, Faculty Handbooks, New Classified Employee Handbook, and the Handbook for New Administrators. Copies of this Policy are also available in the District Human Resources Office, the Office of the Dean of Student Development and EOPS (De Anza), the Office of the Dean of Student Affairs and Activities (Foothill), and on the District's Web site at http://www.fhda.edu.~~

~~Enforcement of the Policy~~

~~The Board directs the Chancellor or designee to enforce all existing federal and state laws and District and college policies, including not only those laws and regulations that are specific to computers and networks but also those that apply generally to personal conduct. Violations of this Policy will be dealt with in the same manner as violations of other District policies or standards of behavior and may result in disciplinary action, subject to applicable due process requirements.~~

~~Users who believe this policy has been misinterpreted or misapplied may file a complaint in accordance with the Complaint Procedures found in Administrative Procedures 3250.~~

Students who do not observe the requirements of this Policy may be in violation of the Student Code of Conduct and subject to student discipline. **Employees who do not observe the requirements of this Policy may be subject to disciplinary action up to and including termination.**

This Policy and Administrative Procedure ~~3520~~ **3720** shall be distributed to all new and existing employees. Nothing in this policy should be construed to interfere with First Amendment rights or with the academic freedom of faculty as outlined in Board Policy 4190.

References:
Education Code Section 70902;
Government Code Section 3543.1 subdivision (b);
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
17 U.S. Code Sections 101 et seq.

See Administrative Procedure ~~3250~~ ***3720*** ~~*Procedures Regarding Misuse of Computer Information*~~
Computer and Network Use

Approved 11/17/97
Revised 07/07/03, 12/05/05, **XX/XX/23**

RECOMMENDED EDITS

Proce~~dures Regarding Misuse of Computer Information~~ Computer and Network Use

AP ~~3250~~ 3720

This administrative procedure implements Board Policy ~~3250~~ **3720**.

The Computer and Network Use Policy ("the Policy") applies to all members of the District community using the District Network including faculty, administrators, staff, students, independent contractors, and authorized guests. The Procedure covers the use of computer equipment and communication systems at any District facility in computer labs, classrooms, offices, and libraries, and the use of District equipment, servers, systems, and networks from any location. If any provision of this Procedure is found to be legally invalid, it shall not affect other provisions of the Procedure as long as they can be effective without the invalid provision.

Ownership Rights

The Procedure is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, and all hardware and software components within it, is the sole property of the District which sets the terms and conditions of its use consistent with the law. Except as provided in Board Policies, Administrative Procedures, and collective bargaining agreements pertaining to intellectual property rights, network users have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the District Network.

Privacy Interests

The District recognizes the privacy interests of faculty and staff and their rights to freedom of speech, participatory governance, and academic freedom, as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of the District's business make electronic communication less private than many users anticipate and may be subject to public disclosure. In addition, the District Network can be subject to authorized and unauthorized access by both internal and external users. For these reasons, there are no online activities or services that guarantee an absolute right of privacy, and therefore, the District Network is not to be relied upon as confidential or private. Nonetheless, the District seeks to afford email communications privacy protections comparable to those it traditionally affords paper mail and telephone communications consistent with state and federal laws.

District Rights

System administrators may access user files or suspend services they manage without notice: 1) to protect the integrity of computer systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; or 4) when it is reasonable to believe that violations of law or District policy or Administrative Procedures have occurred. For example, system administrators, following District guidelines, may access or examine individual files or accounts based on suspicion that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board Policy or Administrative Procedure and/or to protect system integrity. Such data or information may also be used as grounds for appropriate disciplinary action.

Access to the District enterprise resource planning ("ERP") system or other District applications or databases containing personally identifiable information ("PII") or protected health information ("PHI"), or any other student or employee information protected by state or federal law, shall be granted upon the successful completion of the Department of Justice ("DOJ") Live Scan fingerprint check.

To ensure an effective response to emergency situations, the District may monitor telephone calls only when an emergency call is made to 911. This emergency call monitoring allows District Police to communicate and coordinate with Police, Fire, and other emergency responders.

User Rights

While the District uses automated processes to monitor electronic usage as part of its normal network operating procedures, the District does not routinely inspect or monitor individual users' computer hardware or files, email, and/or telephone messages, nor disclose information created or stored in such media without the user's consent unless required by law. The District shall attempt to notify users before accessing computer hardware and files or prior to suspending service. If the District acts without user consent, under its District Rights specified above, the District shall do so with the least perusal of contents and the least action necessary to resolve the immediate situation. When the District accesses files without user consent, it shall notify the user as soon as possible of its access and provide the reason for its action.

User Responsibilities

The District recognizes that computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, policies, procedures, and contractual obligations.

For District employees, the intended uses of the District Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional or other authorized activities.

"Unauthorized uses" include prohibited uses and any other use for a prohibited purpose, including illegal activities, messages which may constitute discrimination or harassment under state or federal law, or anything that interferes with the intended use.

No Personally Identifiable Information (PII) unrelated to district matters should be stored or transmitted using the District Network. Users are prohibited from receiving, transmitting, or storing student or employee information categorized as PII outside District systems specifically designated for secure storage and transmittal of PII.

Users accessing the District Network are expected to act responsibly and engage in safe computing practices. To protect the integrity of the District Network and the information it contains, all employees are provided with regular cybersecurity training modules and should utilize effective cybersecurity practices.

International Travel

When traveling outside the United States, employees will be restricted from accessing certain sensitive data systems and/or connecting to the District Network via Virtual Private Network (VPN) connections. These limitations are intended for security purposes and the District will make an effort to allow international access to instructional systems to the greatest extent feasible given security, data protection, and risk considerations. Additionally, when engaging in authorized international travel, employees shall ensure District-owned computing hardware and any storage devices containing District data are encrypted per current District standards.

All District Network users must read, understand, and comply with this Administrative Procedure, Board Policy 3720, and any additional guidelines established by the District. Such guidelines will be reviewed by the District and may become subject to Board approval as a District policy or procedure. By using any part of the District Network, users agree that they will comply with this Procedure.

Copies of this Policy can be found in the policies section of the College Catalogs, Schedule of Classes, Student Handbooks, Faculty Handbooks, New Classified Employee Handbook, and the Handbook for New Administrators. Copies of this Policy are also available in the District Human Resources Office, the Office of the Dean of Student Development and EOPS (De Anza), the Office of the Dean of Student Affairs and Activities (Foothill), and on the District's web site at http://www.fhda.edu.

Enforcement of the Procedure

The Chancellor or designee will enforce all existing federal and state laws and Board Policies and Administrative Procedures, including not only those laws and regulations that are specific to computers and networks but also those that apply generally to personal conduct. Users violating Board Policy 3720 and this Administrative Procedure will be dealt with in the same manner as violations of other Board Policies or Administrative Procedures or standards of behavior.

Users who believe this policy has been misinterpreted or misapplied may file a complaint in accordance with the Complaints procedures found below.

Students who do not observe the requirements of this Procedure may be in violation of the Student Code of Conduct and subject to student discipline. Employees who do not observe the requirements of this Procedure may be subject to disciplinary action up to and including termination. Such violations may also be subject to criminal investigation when warranted.

The District is responsible for making this Procedure readily accessible to all users prior to their use of the District Network. Abuse of computing, networking or information resources contained in or part of the District Network may result in the loss of ~~computing privileges~~ **access to the District Network**. Additionally, abuse can be prosecuted under applicable ~~statutes~~ **laws**. Users may be held accountable for their conduct under any applicable **Board**, District or College policies, **Administrative** Procedures, **state and federal laws**, or collective bargaining agreements. Complaints alleging abuse of the District Network will be directed to those responsible for taking appropriate disciplinary action. Illegal reproduction of material protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.

~~Examples of behaviors constituting abuse which violate District Board Policy 3250 include, but are not limited to, the following activities:~~

System Abuse

Examples of behaviors constituting abuse include, but are not limited to, the following:

- **Any activity which is illegal.**
- Using a computer account that one is not authorized to use.
- Obtaining a password for a computer ~~account~~ **or application or system** that one is not authorized to have.
- Using the District Network to gain unauthorized access to any ~~computer~~ **information technology** systems.
- Knowingly performing an act which will interfere with the normal operation of ~~computers, terminals, peripherals or networks~~ **applications, systems, computers, terminals, peripherals, or networks**.
- Knowingly running or installing on any ~~computer~~ system or network **a program intended to take control of the computer(s) systems** or giving to another user a program intended to damage or to place excessive load on a computer system or network. **This includes programs known as computer viruses, Trojan horses, zombie software, and worms.**
- Knowingly ~~or carelessly~~ **or through negligence** allowing someone else to use your account ~~who engages in any misuse in violation of Board Policy 3250 or of this AP3250~~.
- Forging e-mail messages.
- Attempting to circumvent data protection schemes or uncover or exploit security loopholes.
- Masking the identity of an account or machine.
- Deliberately wasting computing resources, **such as by engaging in file sharing schemes, participating in e-mail chains, spamming, and/or excessive bandwidth usage**.
- **Intentionally accessing**, downloading, displaying, uploading, or transmitting obscenity or pornography, as legally defined.
- Attempting without District authorization to monitor or tamper with another user's electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal ~~under California Computer Crime Laws~~.
- Personal use, which is excessive or interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the Network.
- Illegal downloading and/or distribution of copyright-protected materials, including music and videos.
- **Using the District Network for online gambling.**
- **Using the District Network for political purposes as set forth in Education Code Section 7054.**

Harassment

- Using the **District Network, including** telephone, e-mail, voicemail, **or other electronic communications**, to harass or threaten others.
- Knowingly downloading, displaying, or transmitting by use of the District Network, communications, pictures, drawings, or depictions that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political belief.
- Knowingly downloading, displaying, or transmitting by use of the District Network sexually explicit images, messages, pictures, or cartoons ~~when done to harass or for the purposes of harassment~~ **which have the clear purpose of harassment or have been identified as harassment as the result of a formal investigation into the matter.**

- Knowingly downloading, displaying, or transmitting by use of the District Network sexually harassing images or text ~~in a public computer facility, or location that can potentially be in view of other individuals~~ **that do not constitute proper exercise of academic freedom or constitutionally protected free speech or expression within a public computer facility or location that can potentially be in view of other individuals.**
- Posting on ~~electronic bulletin boards~~ **sites or applications** material that violates existing laws or the colleges' Codes of Conduct.
- Using the District Network to publish false or defamatory information about another person.

Commercial Use

- Using the District Network for any commercial activity, **other than incidental or traditional commercial use**, without written authorization from the District. "Commercial activity" means for financial remuneration or designed to lead to financial remuneration. **Examples of "incidental or traditional commercial use" include but are not limited to:**
    - **Electronic communication between an instructor who is an author of a textbook and his/her publisher.**
    - **Electronic communication by a staff member who uses the District Network to communicate regarding a presentation at an educational conference or workshop for which that staff member might receive an honorarium.**
    - **Electronic use of the District Network by a student to seek a part-time or full-time job or career related to the student's field of study, or to assist her/him in applying for such work.**
    - **Electronic communication by a staff member to inform a colleague about their child's candy bar fundraising sale for the child's school.**
    - **Using electronic resources to research and/or purchase supplies, equipment, or other items required for campus, District, or student use.**

Copyright

- Violating terms of applicable software licensing agreements or copyright laws.
- Publishing copyrighted material without the consent of the owner on District web sites in violation of copyright laws.
- **Downloading of unlicensed or copyrighted movies or music for other than legally authorized uses or uses authorized by the District.**
- **Illegally downloading copyrighted material or information that would enable the unauthorized utilization of copyrighted material.**

Exceptions

The interaction of a user's personal computing equipment, connected to the District Network, is subject to this Procedure. Contents of a user's personal computing equipment are subject to search by the District only by legal warrant.

There may be times when District employees may be exempted from certain provisions of this Procedure to perform their duties or assignments that are an established part of their job.

Activities by technical staff, as authorized by appropriate District or College officials, to take action for security, enforcement, technical support, troubleshooting or performance testing purposes will not be considered abuse of **the District** Network.

Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities and will take no disciplinary action provided that such use is within reason and provided that such usage is ordinarily on an employee's own time; is occasional, ~~and~~ does not interfere with or burden the District's operation, **and is not otherwise contrary to Board Policies or Administrative Procedures**. Likewise, the District will not purposefully surveil or punish reasonable use of the District Network for union business-related communication between employees and their unions.

Complaints by Employees or Students Regarding Enforcement of this Procedure

An ~~user~~ **employee** who asserts that the District or District personnel have violated this ~~policy~~ **Procedure** ~~shall~~ **may alert the Vice Chancellor of Technology or any ETS manager of the incident and may also** file a complaint with ~~his or her immediate supervisor with a copy to~~ the Vice Chancellor of Human Resources **and Equal Opportunity**, ~~and~~ **with** a copy to the employee's bargaining unit **if applicable**. The ~~supervisor~~ **appropriate manager** shall notify the supervisor of the alleged violator to discuss the complaint. ~~The supervisor of the complainant~~ **District management** shall initiate an investigation if necessary and determine an appropriate remedy/resolution in consultation with the Vice Chancellor of Human Resources **and Equal Opportunity and/or the Vice Chancellor of Technology**. In cases where the supervisor is part of the complaint, the complaint shall be filed with the next level of supervision for investigation and resolution and/or remedy. The complainant shall be informed in writing 1) of the initiation of the investigation, and 2) of its outcome as appropriate, with copies to the Vice Chancellor of Human Resources **and Equal Opportunity** and the employee's bargaining unit **as applicable**. Complainants dissatisfied with the resolution/remedy have full recourse to relevant contractual protections and/or legal action.

A student who asserts that the District, its personnel, or another student has violated this Procedure may alert college or district personnel, who may take appropriate action and shall immediately notify the Vice Chancellor of Technology regarding the specifics of the incident. If the student deems it necessary, they may file a complaint pursuant to the College's student complaint process.

References:
Government Code Section 3543.1 subdivision (b);
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
15 U.S. Code Sections 6801 et seq.;
17 U.S. Code Sections 101 et seq.;
16 Code of Federal Regulations Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45;

*See Board Policy ~~3250~~ **3720** ~~Computer Use: Rights and Responsibilities~~* ***Computer and Network Use***

Approved 11/17/97
Reviewed 08/16/99, 07/07/03
Revised 10/28/05, 02/06/09, **XX/XX/23**