



*Club Name : _____

*Short Name : _____ *College : _____

*Advisor Name : _____ *Department : _____

*E-Mail / Phone : _____

Club Officers :	Name (Print) :	Student ID :	Signature :
-----------------	----------------	--------------	-------------

*President :	_____	_____	_____
--------------	-------	-------	-------

*Vice President :	_____	_____	_____
-------------------	-------	-------	-------

*Secretary :	_____	_____	_____
--------------	-------	-------	-------

*Treasurer :	_____	_____	_____
--------------	-------	-------	-------

*ICC Rep. :	_____	_____	_____
-------------	-------	-------	-------

Other Members who will have access to e-mail account:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

All fields with an "*" are required for approval of club e-mail account.

E-mail Account Format:

- Club e-mail accounts will use the format college.club.shortname. For example:

sbvc.club.psychology@student.sbccd.net
chc.club.psychology@student.sbccd.net

Agreement Guidelines:

- Student club e-mail accounts will be deactivated at the end of the spring semester, and this form must be resubmitted before re-activation is allowed.
- Inter Club Council (ICC) can suspend a club e-mail account based on : **1) Inactive / Active Status. 2) Inappropriate content.**
- District and/or College can suspend a club e-mail account based on board policies and inappropriate use.
- Full responsibility for management of the club e-mail account is that of the club advisor.
- Only those listed and have signed above are allowed to access the club e-mail account, or be able to request support from the help desk.

By signing, I hereby declare that I have read and agree to abide by the attached guidelines.

Note: The attached guidelines and SBCCD policies relating to student e-mail can be access online at <http://student.sbccd.net/disclaimer.wssp> and district policies at <http://www.sbccd.org/index.php?CurrentDir=Board/Policies/>.

_____	_____
Club Advisor	Date

_____	_____
ICC Commissioner	Date

_____	_____
Coordinator of Student Activities	Date

ACCEPTABLE USE POLICY
For the Computer Resources at
San Bernardino Community College District

October 2000

1.1 GENERAL PRINCIPLE:

The computer resources of the San Bernardino Community College District are for the use of persons legitimately affiliated with SBCCD (as faculty, staff, students, or administrators) to facilitate the exchange of information consistent with the academic, educational and research purposes. Specifically, the district computer users have access to:

- 1) Electronic mail communication with people all over the world.
- 2) The World-Wide Web and the information contained therein.
- 3) Discussion groups on a plethora of topics
- 4) Many College Library Catalogs, the Library of Congress and ERIC.

Every SBCCD computer user is responsible for being aware of these guidelines, and is expected to follow these guidelines, both in letter and in spirit. It is a general policy that all computers are to be used in a responsible, efficient, ethical and legal manner. Failure to adhere to the policy and the guidelines below will result in appropriate disciplinary action, up to and including termination.

SPECIFICALLY ACCEPTABLE USES:

- Conducting the business of the district.
- Developing and preparing classroom material.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub field of knowledge.
- Use for disciplinary-society, college-association, government-advisory, or standards activities related to the user's research and instructional activities.
- Use in applying for or administering grants or contracts for research or instruction, but not for other fundraising or public relations activities.
- Any other administrative communications or activities in direct support of research and instruction.
- Announcements of new products or services for use in research or instruction, but not advertising of any kind.
- Communication incidental to otherwise acceptable use, except for illegal or specifically unacceptable use.

1.2 UNACCEPTABLE USES:

- Accessing computers, accounts or folders, other than those specifically authorized by your supervisor, or District computer services.
- Intruding into any system in such a way as to diminish the effectiveness of system performance.
- Use for for-profit activities.
- Extensive use for private or personal business.
- Advertising is forbidden. Discussion of a product's relative advantages and disadvantages by users of the product is encouraged.

2. E-mail

The E-mail at SBCCD is here to provide a convenient (not confidential) way of communicating between students, faculty, staff, administrators and professional colleagues. It is expected that SBCCD computer users will use common courtesy in the use of E-mail. Specifically, the following activities are not acceptable:

- Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the network. Therefore, messages should not contain profanity, obscene comments, sexually explicit material, and expressions of bigotry or hate.
- "Chain letters," "broadcasting" messages to lists or individuals, and other types of use, which would cause congestion of the networks or otherwise interfere with the work of others are not allowed.

3. Software Licensing

All commercial software used on college computers must be licensed to the college or to the individual who is using the software. Individuals should be prepared to show their department manager a license for the software on any college computer. NOTE: All software should be assumed to be commercial unless otherwise noted. The district has the capability to electronically monitor the software install on all district computers. The district reserves the right to do this.

3.1 District-wide software Licenses

SBCCD has obtained favorable site licenses for many products. For a list of software that is licensed to the district see the District Computing Services office. At the time of printing (July, 2000) this software includes (MS Office Suite, MS Front Office products, MS operating systems, McAfee Virus protection software.)

3.2 Departmental software Licenses

Individual departments can purchase software for use by the employees of that department. License information should be kept in the departmental office and be available for examination if required by a college, district or law enforcement official.

3.3 Individual Software Licenses

The district is responsible for providing access to all software necessary in the performance of ones duties. Employees are not to install individual software on their computers. Any fines levied for pirated software will be paid by the individual who regularly uses the computer.

STAFF

All software necessary to do your job has been installed on your computer by the District Computer Services office. No additional software should be added to your system.

FACULTY

From time to time faculty may need to install software on their primary computer. This software must be licensed to the individual or the department. All appropriate license fees should be paid. This software must be reported to the appropriate departmental manager.

STUDENTS

No students shall install software on any district/college computers, except as authorized by the instructor in the course of learning.

4. Security

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on any of the district computers, you must notify the system administrator. Do not demonstrate the problem to other users.

4.1 Usernames, Passwords, Personal Identification Numbers (PINS)

Students and employees may be issued usernames, passwords and/or PINs.

- 1) These electronic IDs are unique to the individual and should be guarded carefully.
- 2) These IDs and its associated rights will give the user of the ID access to certain data, files, information and resources within the district's electronic resources.
- 3) These IDs will be treated as electronic signatures and carry the same authority as a written signature when used in conjunction with district or college documents, screens, telephone systems or web forms. (THEREFORE, guard your electronic IDs carefully.)
- 4) If you believe someone else is using your ID, contact the systems administrator immediately.

4.2 Data Security Policy

- Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Users shall not misrepresent other users on the network.
- Users shall not attempt to gain unauthorized access to data, system programs or computer equipment.
- Users must not give their password to another user
- Users should change passwords frequently. The system will enforce password changes every 90 days. But you may change more frequently if you feel it is necessary.

4.3 Network Security Policy

Network Security is and should be the responsibility of every individual who uses the District's computing resources. All managers and technical employees should be especially aware of the possible vulnerabilities. District Computing Services is responsible for maintaining security through the issuing of passwords, and administration of all access points into the "Secured" network. No deviations should be made to these security measures without the written permission of the Director of District Computing Services or his/her designee. District Computing services will issue Network Security Guidelines that will dictate appropriate security measures on the computer systems. All computing personnel in the district are responsible for familiarizing themselves with the guidelines. Strict adherence to these guidelines is expected. Any breach of security may be a condition of continued employment. (See Appendix A for current Network Security Guidelines.)

5. Privacy

District employees will act in accordance with the Data Access Guidelines when accessing district data.

Please remember:

- All data stored on the district's computer systems belong to the district. Therefore, no user should expect that this data is private.
- Electronic Mail (e-mail) is a form of public communication and cannot be guaranteed to be private. Be discreet.
- People who operate the system do have access to all files stored on the district's servers. From time they may be required to, in the performance of their jobs, access data or files stored on any of the district's computers. The computing staff will examine or disclose the contents of files only when authorized by the owner of the information or by the district's Chief Information Systems Officer, in conjunction with the appropriate Cabinet-level official (Chancellor, or one of the Vice Chancellors, Presidents, or Vice Presidents.)

6. Vandalism

Vandalism is defined as any malicious attempt to harm, modify, or destroy computer hardware, data of another user, SBCCD, or any of the other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses. In all cases, policies regarding vandalism will apply.

7. Access to Institutional Data

Employees of the district should treat all data stored on central computers as secure. This data should only be accessed in accordance with the Data Access Guidelines that are developed by the Data Access Committee. These guidelines apply to all district data (as defined in the Data Access Guidelines) and are intended to provide the appropriate combination of security and access. The policy does not apply to notes and records that are the personal property of individuals in the district community, and is not directed to data whose primary purpose is scholarly (instructional material, research notes, etc.). In all cases applicable statutes and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy. (See appendix B for sample Data Access Guidelines)

8. Access to World-wide Data

Faculty, staff and students will have access to the Internet, the World-Wide Web, and all related resources, from most district computers. It is intended that the Internet will be used to conduct official college business or in the pursuit of scholarship. Any restrictions on the use of the Internet by faculty, staff or students will be made either by college, departmental or office procedures.

Appendix A

Network Security Guidelines

These guidelines will be modified from time to time by the District Computing Services in consultation with District and College management, and college computing personnel.

The following guidelines help ensure that only authorized users will have access to the College and District's secured data.

- 1) The network backbone on the colleges has been divided into two different and distinct networks: the Trusted Network (Secured) and the Open Network (Unsecured).
- 2) All computers regularly used by students of the Colleges or accessible to the general public are and should be placed in the Open network. These computers and their authorized users have access to the various web servers, academic support software, faculty distribution files, etc.
- 3) All computers regularly used by employees of the District, and not generally available for student use, should be and are placed in the Trusted network. In addition to having access to all of the resources of the Open network, these computers and their authorized users have physical access to campus e-mail systems, file servers, print servers and the central databases (Student Information System).
- 4) All employees of the District who make regular use of the computer systems are issued passwords to the network. These passwords should be treated as confidential and never released to anyone.
- 5) If someone who is not a regular employee of the District (e.g. part-time or student workers) has need of a password, this authorization can be provided by a district/college manager AND the Director of District Computing Services.
- 6) Computers on the Trusted Network shall not be made available to the Open Network. The following activities would do that and are not allowable:
 - a) Installing a hub, switch or router that would connect both the Open and Trusted network.
 - b) Installing dual cards into a computer that would connect one to the Open Network and one to the Trusted network.
 - c) Using a modem connection to connect to the Internet from the Trusted Network.
 - d) Installing a modem and running remote access software (e.g. PC Anywhere).
 - e) Using a major ISP's Internet software to connect to your service. (e.g. AOL, CompuServe, etc.) This does not include using the Web and the campuses Internet connection to access e-mail, or Web-enabled services, this only includes using the software provided by the vendor to access these services while you are on campus. (There are known security flaws in these packages which will open our system up to hacker attack.)

APPENDIX B
Guidelines for Institutional Data

(This is a sample policy, which will not become effective concurrent with the Computer Use policy)

STATEMENT OF POLICY

Access to institutional data -- the permission to view or query institutional data -- should be granted to all eligible employees of SBCCD for legitimate district purposes.

Each data item and each view of that data item will be assigned to one of three categories: public, district-internal, or limited-access.

Except, as noted below, all institutional data will be designated as district-internal data for use within the district. All eligible employees of the district will have access to these data, without restriction or prior authorization, for use in the conduct of district business. These data, while freely available within the district, are not open to the general public.

As appropriate, data stewards may identify data elements or views that have no access restriction whatsoever and that may be released to the general public. These will be designated public data.

As necessary, data stewards may designate some data elements limited-access data. Such designation will include: specific reference to the legal, ethical, or other constraint that requires this restriction and description of the categories of data users that are typically given access to the data, the conditions under which access is given, or the limitations that apply to such access.

Data stewards will work together with the District's Chief Information Systems Officer to define a single set of procedures by which users may request permission to access limited-access institutional data, and will be jointly responsible for documenting these procedures. Each data steward will be individually responsible for documenting data access procedures that are unique to a specific information resource or set of data elements.

Any data user may request that a data steward or the committee of data stewards as a group review the restrictions placed on a data element or data view, or review a decision to deny access to limited-access data. When necessary, the Committee on Institutional Data will make the final determination on data restrictions and requests for access rights to institutional data.

Data users will be expected to access institutional data only in their conduct of district business, to respect the confidentiality and privacy of individuals whose records they may access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information. Expressly forbidden is the disclosure of limited-access or district-internal institutional data or the distribution of such data in any medium, except as required by an employee's job responsibilities. Also forbidden is the access or use of any institutional data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's own personal curiosity. Violation of this policy will be dealt with seriously. Violators will be subject to the normal disciplinary procedures of the district and, in addition, the loss of data access privileges may result.

Data Access Committee (DAC). Chaired by the District's Chief Information Systems Officer, this committee establishes overall policy and guidelines for management and access to the institutional data of the district. The members of this committee shall consist of, but not be limited to, the colleges' director of records, the District's Director of Human Resources, and one representative from each campuses faculty, and can include all individuals identified as Data Stewards.

Data, institutional. A data element is considered institutional data if it satisfies one or more of the following criteria: it is relevant to planning, managing, operating, or auditing a major administrative function of the district; it is referenced or required for use by more than one organizational unit; it is included in an official district administrative report; or it is used to derive an element that meets the criteria above. The data steward, under the oversight of the DAC, will apply these criteria to determine which data are institutional in nature. Any data steward, data

manager, user group, or data user may identify and suggest data elements for consideration by the committee of data stewards.

Data, limited-access. These are data elements that, because of legal, ethical, or other constraints may not be accessed without specific authorization or to which only selective access may be granted.

Data, public. These are data elements to which the general public may be granted access.

Data, district-internal. These data elements may be accessed by all eligible employees of the district, without restriction, for the conduct of district business. Without further indication, all data elements stored on district computers will be designated "District-internal data."

Data access, institutional. Access to institutional data refers to the permission to view or query data.

Data managers. District officials and their staff who have operational-level responsibility for data capture, data maintenance, and data dissemination.

Data stewards. District officials who have policy-level responsibility for managing a segment of the district's information resource.

Data users. Employees (full-time, part-time and students employees) of SBCCD who access institutional data in performance of their assigned duties.

Colleague Screen. A logical collection of data elements, possibly from multiple physical databases, that are assembled and presented according to a defined set of rules.

Eligible employees. Faculty, staff and administrators holding full-time appointment in the District or other employees specifically designated as eligible by the head of their department, division, school, or campus.

COMPUTER USE POLICY

In support of the mission of the District's colleges to educate those in their respective service areas, the colleges provide computing, networking, and information resources to their students, faculty, and staff.

A. Rights and Responsibilities

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 laws, regulations, and contractual obligations.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, District administrators may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines, administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

B. Existing Legal Context

All existing laws (federal and state) and regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal contact.

Misuse of computing, networking, or information resources may result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable college or District policies, procedures, or collective bargaining agreements. Complaints alleging misuse of the District's technological resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Activities will not be considered misuse when authorized by District officials or those contracted by the District for security or performance testing.

C. Additional Use Policies

Additional use policies and terms and conditions may be in place for specific electronic services offered either by the colleges or by the District. *This information will be included in Administrative Regulations, computer lab regulations, or faculty developed regulations for class operation.*

D. Enforcement

Penalties may be imposed under one or more of the following: Policies and regulations publicized in the *Administrative Regulations*, college catalogs, California law, or laws of the United States.

Reference:
Education Code § 70902
ADOPTED: 7/12/01
AMENDED: 4/8/04