IMPERIAL COMMUNITY COLLEGE DISTRICT
AP 3720 Computer and Network Use

References: 17 U.S. Code Sections 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 and network systems are the sole property of Imperial Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

This procedure applies to all District students, faculty and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

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 or restrictions.

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 users 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 way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Copyrights – In addition to software, all other copyrighted information (text, images, icons, programs, 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 or any other protected work is prohibited.

Integrity of Information Resources
Computer users must respect the integrity of computer-based information resources.

Modification or Removal of Equipment – Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

Unauthorized Use – Computer 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, wither 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 available; 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 - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users 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 may further lead to civil or criminal legal proceedings.

Unauthorized Access - Computer users 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 system administrator so that steps can be taken to investigate and solve the problem.

Password Protection – A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

Usage - Computer 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 the District procedure and may violate applicable law.

IVC Email Access – Newly hired regular/contract employees and part-time faculty will be provided IVC account access upon job acceptance and notification from HR. If a newly hired regular/contract employee or part-time faculty rescinds a job offer or becomes ineligible for employment, HR will notify IT to revoke the access immediately.

Temporary employees will be provided IVC account access as follows:

- Professional experts who are employed for 90 days or longer as requested by the hiring department administrator.
- Temporary hourly Substitute Employees as requested by the hiring department administrator
- Student workers who do not have an assigned student IVC access will be provided access upon request by the hiring department administrator
- Volunteers will normally not be provided IVC account access
- All temporary employees will have their IVC account access removed upon termination from the District

Regular/Permanent Employees who separate from the District will have their IVC account access removed within 48 hours of departing the District. By exception, the CTO or CHRO may approve continued IVC account access for a period of time.

Employees who leave the District for cause will have their IVC account access removed immediately. The CHRO will notify the employee and CTO of any such circumstance. An employee who departs the District for cause may request from the CHRO temporary access to their locked account to remove any personal files or documents.

Part-Time faculty who depart the District or are not provided an assignment for a period of 24 months will have their IVC account access removed.

HR will conduct periodic audits of employee status and account access, and update IT department of any IVC account access which needs to be removed based on the above stated parameters.

Any employee found using the IVC email account inappropriately is subject to having their access revoked.

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

Commercial Usage – Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public discussion groups have been designated for selling items by IVC OpenComm and may be used appropriately, according to the stated purpose of the group(s).

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

Rights of Individuals – Users must not release any individual's (student, faculty, or 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.

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 District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.

Commercial Use - District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

Nondiscrimination
All users have the right to be free from any conduct connected with the use of Imperial Community College District network and computer resources which discriminates against any person on the basis of an ethnic group identification, gender, gender identity, gender expression, genetic information, pregnancy, race, color, national origin, religion, age, sex, physical disability, mental disability, ancestry, sexual orientation, language, accent, citizenship status, transgender status, parental status, marital status, economic status, veteran status, medical condition, or on the basis of these perceived characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics (See AP 3410).

No user shall use the District network and 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 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 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.

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

Dissemination and User Acknowledgment
All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

A “pop-up” screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The “pop-up” screen shall appear prior to accessing the e-mail network. Users shall sign and date the acknowledgement and waiver included in this

procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgement and waiver shall be in the form as follows:

Computer and Network Use Agreement

I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.