

## 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.

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.

Nondiscrimination

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