32793
ADOPTED – BOARD OF TRUSTEES
COMMUNITY COLLEGE DISTRICT NO. 508
OCTOBER 1, 2015

BOARD OF TRUSTEES OF COMMUNITY COLLEGE DISTRICT NO. 508
COUNTY OF COOK AND STATE OF ILLINOIS

RESOLUTION
ADOPTING REVISIONS TO ARTICLE 6 OF THE BOARD POLICIES AND PROCEDURES
OFFICE OF INFORMATION TECHNOLOGY

WHEREAS, the Board of Trustees of Community College District No. 508 is empowered under Section 805/3-30 of the Illinois Public Community College Act, 110 ILCS 805 ("the Act") to exercise all powers not inconsistent with the Act, "that may be requisite or proper for the maintenance, operation and development of any college or colleges under the jurisdiction of the board";

WHEREAS, Section 4.3 of the Board Bylaws provides that the Board may adopt, from time to time, policy statements, guidelines, procedures, regulations, collective bargaining agreements, codes of conduct, or similar documents issued for the governance of the Board, the District and the Colleges;

WHEREAS, the Office of Information Technology has determined that a revision to Article 6 of the Board Policies and Procedure Manual is necessary to assist the District in maintaining efficient operations and management flexibility; and

WHEREAS, the Chancellor supports the recommendation of the Office of Information Technology;

NOW THEREFORE BE IT RESOLVED, that the Chancellor recommends that the Board of Trustees approves the amendment to Article 6 of the Board Policies and Procedures (See Exhibit A – Executive Summary, Exhibit B – Proposed Revisions and Exhibit C – Revisions to Article 6). Said policy revisions will be reflected in updated publications of the Board Policies and the City Colleges of Chicago website and shall be effective immediately.

October 1, 2015 – Office of Information Technology

EXHIBIT A

EXECUTIVE SUMMARY
PROPOSED REVISIONS TO ARTICLE 6 OF THE
BOARD POLICIES AND PROCEDURES FOR MANAGEMENT & GOVERNMENT

The policy revisions to Article 6 are summarized below, and apply to all District employees, students and guests of CCC technologies.

References to Information systems has been replaced with technologies throughout the document.

6.0 Introduction
Added new introduction.

6.1 Scope of Policy
The proposed policy revision includes additional circumstances to the use of technologies in the CCC environment.

6.3 Authorized Uses
The proposed policy revision includes additional circumstances to the authorized uses of technologies in the CCC environment.

6.4 A. Harassment
The proposed policy revision expands this section to include any other inappropriate behavior that would be offensive to others.

6.4 B. Capacity Used
The proposed policy revision states that CCC can impose controls and limits for network bandwidth.

6.4 F Protection of Card Holder Data
New Policy

6.6 Security
The proposed policy revision includes additional circumstances to security and audit practices.

6.7 Additional User-Specific Provisions #4 Authorized Agency Connection
The proposed policy revision states that third party providers cannot connect to the CCC network directly.

6.7 Additional User-Specific Provisions #7 Electronic Transmissions
New Policy

6.8 Enforcement
The proposed policy revision explains the repercussions of non-adherence to the policy.

EXHIBIT B

ARTICLE 6
INFORMATION TECHNOLOGY

6.0 INTRODUCTION

The Acceptable Use Policy applies to all users of the City Colleges of Chicago (CCC) technologies, whether affiliated with the CCC or not, and to all Users of those resources, whether on campus or from remote locations.

The Office of Information Technology (OIT) is responsible for the governance and the setting of technology standards, operating guidelines, acquisition, maintenance, and the decommissioning of all CCC technologies throughout the District Office and the Colleges.

CCC provides technology resources for use by students, faculty, employees and guests to support academic and administrative functions and services.

The Acceptable Use Policy is in place to protect and safeguard CCC's technology assets and ensure performance and throughput is not impeded by unacceptable activity and use.

All users of CCC's technologies must comply with the Acceptable Use Policy. Those who fail to comply could be subject to disciplinary action or referral to the appropriate legal authorities (Refer to Section 6.8 Enforcement).

6.1 SCOPE OF POLICY.

This policy is applicable to all users of CCC technologies. CCC technologies includes but is not limited to networks—Ethernet and Wi-Fi; telephones and telecommunications equipment; computer tools; applications; systems; data and databases; academic and advising systems; internal and external websites; cloud-based or hosted systems and services; e-mail; shared drives; collaborative work sites (including SharePoint); data warehouse; analytics systems; mobile apps, systems, sites and data; computers, desktop workstations, laptops, notebooks, and ultra-books; loaner laptops; tablets; iPads; printers; computer labs; smart boards; projectors; and classroom devices; facsimile (FAX) machines; simulator devices; and any associated peripherals, or any software regardless of whether used for administrative, research, teaching, personal or other purposes.

While CCC allows the use of personally-owned internet connectable devices (smart/mobile phones, PDAs, tablets, notebooks, laptops, and other devices), the Acceptable Use Policy also extends to the use of these devices whenever they use CCC data and/or networks through wired or wireless connections. Personally owned computers and mobile devices may be restricted from accessing certain highly secured CCC applications, systems and internal Wi Fi networks.

This policy refers to the use of technologies whether owned, leased, operated, controlled, installed or otherwise furnished by CCC. CCC technologies may be in buildings, fixed outdoor or mobile locations such as buses and vehicles used by students, employees and guests.

6.2 LEGAL COMPLIANCE.

All users of CCC's technologies must comply with all federal, Illinois, and other applicable laws; all generally applicable CCC rules and policies, including, but not limited to those which apply to personal conduct and those specific to computers, networks, other technologies and all applicable contracts and licenses. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses. All users shall abide by the following provisions contained herein, or otherwise may be subject to disciplinary action or referral to the appropriate legal authorities for failing to comply.

6.3 AUTHORIZED USES.

All users shall confine their use of CCC's technologies to be consistent with what has been authorized. Ability to access technology resources does not, by itself, imply authorization to do so. All users are to protect the security of CCC systems, the confidentiality and privacy of CCC students, employees and records.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. CCC technology accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information violates CCC's policy and may violate applicable law. Technology resources must be used in ways that do not disrupt; or interfere with access; or the operations of these systems and resources.

No one, other than authorized personnel for authorized purposes, shall attempt to modify or remove CCC technology resources or any other computer equipment, software or peripherals that are owned by others without proper authorization from CCC or the owner.

6.4 PROHIBITED CONDUCT.

A. Prohibited Conduct

- CCC's technologies may not be used, under any circumstances, to libel, slander, bully or harass another person.
- It is not acceptable to willfully transmit threatening, obscene, or offensive materials or to knowingly cause such materials to be transmitted. Such as: racial slurs, gender-specific comments, or any other offensive remarks about age, sexual orientation, religious, political beliefs, or national origin
- Sending, receiving or displaying obscene or pornographic text or graphics inappropriate for a public and open environment
- Loading or downloading software from the Internet without prior authorization or using personal owned software programs on CCC computers or network servers
- Installation of personally owned hardware on the network

B. Capacity Used

All users of CCC's technologies shall respect the limited capacity of these resources

and control use not to consume an unreasonable amount of those resources or unreasonably interfere with the activity of other users. CCC reserves the right to give priority to academic, student and administrative functions. This means, at times, controls and limits may be imposed for network bandwidth, service levels, disk storage space and other technical functions and activities. High bandwidth consumption used outside of its intended purpose, may be in violation of this policy.

Users must be good stewards of the technologies offered by CCC. Users rely on shared technology resources simultaneously and, therefore, each user must consider the needs of other users when using these resources. Examples of poor stewardship of technology resources include, but are not limited to: excessive personal use in a lab facility; excessive game playing; streaming videos and movies in computer labs during peak periods, excessive personal use at staff and faculty workstations; continuous running of background programs and reception of large files or running intensive multi-media network applications (digital radio or other media) during high-use times.

C. Illegal File Sharing

Sharing copyrighted materials without a license (i.e., peer to peer file sharing which is often automatically shared) is against the law and also prohibited under this policy and subject to disciplinary action. Copyright abuse can subject both the user and CCC to legal sanctions. Federal law requires CCC to take action when it is notified that someone on its network is distributing copyrighted materials. CCC will not protect any individual users, faculty, staff or students who distribute copyrighted material without a license, nor will it protect or defend individuals who have improperly used CCC technology resources.

D. Personal Gain or Benefit

All users shall refrain from using CCC information systems resources for personal commercial purposes or for personal financial or other gain without proper authorization. All users shall refrain from seeking personal benefit or permit others to benefit personally from any confidential information that has come to them by virtue of their work assignments. Personal use of CCC computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other CCC responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

E. Software License Abuse

CCC requires strict adherence to software vendors' license agreements. Copying of software in a manner not consistent with the vendors' license is strictly forbidden on CCC technologies.

F. Protection of Cardholder Data

CCC maintains Payment Card Industry Data Security Standards (PCI DSS) compliance at all times. PCI compliance requires, among other things:

1. It is prohibited to store sensitive cardholder data [i.e., full account number, expiration date, PIN, and card validation value] on paper or in any system that is not authorized and PCI DSS compliant, including CCC systems, computers, workstations and departmental servers, third-party hosted or in-house software, spreadsheets, cash register systems, e-mail accounts, portable electronic devices (including, but not limited to, laptops, tablets, USB flash drive, PDA, and other external or portable hard drive). Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, clear text, unsecured connections or stored fax.

2. Staff shall not acquire or disclose any information concerning a cardholder's account without the cardholder's written consent.

3. The entire credit card number must not be printed on either the merchant copy or customer copy of any receipts or reports. Old documents with the entire credit card number should have all but the last four digits redacted (blacked out) or be shredded with a cross-cut shredder. Old data files, computer drives and computer media containing credit card information that may exist must be disposed of through a certified destruction company with a receipt of destruction.

4. Any transmission of information that is confidential (e.g. credit card holder data, social security numbers, passcodes etc.).

6.5 PRIVACY.

All users of CCC's technologies shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Ability to access other persons' accounts does not, by itself, imply authorization to do so.

Users should be aware that their uses of the CCC technologies are not completely private and there should be no expectation of privacy. The normal operation and maintenance of CCC's technologies require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. CCC may also specifically monitor the activity and accounts of individual users of CCC technologies, including individual login sessions and communications, without notice, when (a) the user has voluntarily made them accessible to the public; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of CCC or other technologies or to protect CCC from liability; (c) there is reason to believe that the user has violated, or is violating, this policy or any CCC policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law or for any other legally permitted reasons associated with the evaluation, testing, repair or general operation of the CCC technologies.

CCC OIT resources reserves the right to access any CCC systems, any time without notice to maintain, update, upgrade, upload or download software; hosted or on premise.

System administrators will report suspected unlawful or improper activities to the proper

authorities.

CCC, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate CCC personnel or law enforcement agencies and may use those results in appropriate CCC disciplinary proceedings.

Communications made by means of CCC technology resources are also generally subject to the Freedom of Information Act to the same extent as they would be if made on paper.

6.6 SECURITY.

CCC employs various measures to protect the security of its technology resources and of its users' accounts. Users should be aware, however, that CCC cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts and guarding their passwords.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Guidelines. Devices that interfere with other devices or users on the City College's network may be disconnected. OIT security prohibits the installation of software that intentionally blocks authorized scans Firewalls and other blocking technologies must be permitted access to the scan sources.

A. Incident Response

The CCC Incident Response Team (IRT) will receive, review and respond to any and all computer security incident reports and activity including any real or suspected adverse event in relation to the security of CCC computer systems or computer networks. The IRT will review reports, analyze and respond to incidents in accordance with its operating guidelines.

6.7 ADDITIONAL USER-SPECIFIC PROVISIONS

A. Website Reproduction

In addition to fully complying with the Acceptable Use Policy's general provisions, websites housed on CCC web servers (i.e., colleges, departments, faculty, etc.) which reproduce material available over the internet must be done in compliance with all applicable copyright laws. In addition, all CCC information that a school, department or employee desires to post on their websites should only be done with appropriate permission and authority.

B. Third-Party Connections to the CCC Network (vendors, contractors, consultants and external entities)

In addition to fully complying with the general provisions of this policy, all third-party connection users are subject to the following additional provisions:

1. Technology and Systems Protection

Protect the security of CCC systems, the confidentiality and privacy of CCC students, employees and records.

2. Equipment and Resource Inspection
   An inspection is intended to verify that the appropriate level of security is in place as well as verify the existence of proper communication equipment, technical settings, hardware compatibility and anti-virus protection. Any equipment deemed insufficient or risky to the CCC network may be denied access until deemed acceptable. Any external equipment and network devices not made available for the inspection may be disconnected from the CCC network until proper inspection is completed. If any equipment or network device is suspected of endangering network health, performance or security is subject to immediate disconnection.

3. Intruded or Impaired Service
   Any intrusive security audits or tests which may impair the connectivity, functionality and health of the CCC network must be scheduled and approved by the Vice Chancellor/ Chief Information Officer in advance of any such audit or impairment.

4. Authorized Agency Connection
   All third party contractors that provide technology or network support cannot directly connect to the CCC network without approval by OIT in advance. However, if any such connection is authorized, CCC cannot enable the outside agency to compete with any services already provided by agencies with exclusive agreements to provide such services to CCC. Instead, the connection must be limited solely to improving a service provided to CCC.

5. Terminated Connection
   Agencies granted special connections must comply with CCC's Acceptable Use Policy. A violation of the policy will cause immediate termination of connectivity.

6. Internal Connection to Outside Agency
   Any CCC staff requiring a connection to outside agencies must provide a written request to OIT with an explanation of the nature of the desired connection to outside agencies and the benefits expected therefrom.

7. Electronic Transmissions
   Company Information shall be electronically transmitted in a manner consistent with its guidelines. The methods of electronic transmission include e-mail, electronic transfer, text messaging, instant messaging, discussion services, social media, scanners, and facsimile. Internal Use information may be transmitted by e-mail, scanners, facsimile, text messaging or instant messaging.

   Information that is Confidential (such as credit cardholder data) and transmitted internally may require encryption, if requested by the information owner. The information owner will provide the encryption requirements. Confidential Information may NOT be transmitted externally via messaging (text or instant),

discussion service or social media. Confidential Information transmitted externally to any party must either be encrypted or sent over a secure link. Confidential Information solicited by or sent to CCC should be received over a secure link.

C. Community at Large

In addition to fully complying with this policy's general provisions identified here in, all users without access to the CCC network but instead only accessing the internet via CCC's wireless internet service are subject to the following additional provisions:

1. Access to the Service

   The service is a free public service provided by CCC. Your access to the service is completely at the discretion of CCC and your access may be blocked, suspended or terminated at any time for any reason including, but not limited to, violation of this policy, reasons that may lead to liability for CCC or its constituency, disruption of access to other users or networks, and any violation of applicable laws, policies, rules or regulations. All users are subject to the terms of this policy and any future revisions.

2. Acceptable Use of the Service

   Your access to the service is conditioned on your legal and appropriate use of the service. Your use of the service and any activities conducted online through the service shall not violate any applicable law, policy, rule or regulation of the rights of CCC and its constituency.

6.8 ENFORCEMENT.

Violation of the Acceptable Use Policy is very serious. Failure to comply with the Acceptable Use Policy could result in disciplinary actions that could impede a student's ability to excel academically or inhibit an employee in carrying out job duties. These disciplinary actions could include expulsion for a student or termination for an employee and/or referral to the appropriate law enforcement authorities.

All users of CCC's technology resources who are found to have violated any of these policies will be subject to disciplinary action up to and including (but not limited to) warnings, probation, suspension, termination, dismissal, expulsion, and/or legal action. All users, when requested, are expected to cooperate with System Administrators in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files.

Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions. CCC employees should be aware that e-mail on their CCC account and files on CCC computers may be subject to public disclosure under the Illinois Freedom of Information Act. Further, CCC reserves the right to access employee e-mails and files on CCC computers when needed for work-related purposes.

CCC may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of CCC technology resources or to protect CCC from liability.

The CCC Incident Response Team (IRT) will receive, review and respond to any and all computer security incident reports and activity including any real or suspected adverse event in relation to the security of CCC computer systems or computer networks. The IRT will review, reports, analyze and respond to incidents in accordance with its operating guidelines.