Mobile Computing Device Guidelines

North Orange County Community College District (NOCCCD)

Including Fullerton College, Cypress College, the School of Continuing Education and the NOCCCD District Office

Purpose

The purpose of these guidelines is to provide direction for the appropriate usage, including access and support, of Mobile Computing Devices on the NOCCCD network. The network exists to meet the instructional mission of the colleges and district. The guidelines apply to many types of devices including but not limited to Laptops, Smart phones (phones with data/network connectivity capabilities), portable storage devices, tablet devices, and other mobile devices. The key reasons for the creation of these guidelines are:

- to insure uninterrupted support of our instructional mission;
- to protect the District and the colleges from legal liability;
- to meet legal requirements;
- to protect the network so that all can use it;
- to protect the data housed in the systems on the network and;
- to insure that devices can be properly supported for effective use.

Scope

This policy applies to all NOCCCD employees, NOCCCD students and NOCCCD visitors/guests who are authorized by the campus to connect Mobile Computing Devices to NOCCCD's network. The policy sets standards for the purchase, operation, and support of Mobile Computing Devices for NOCCCD employees. This includes any type of handheld communication device capable of transmitting packet data either directly (through NOCCCD's wireless networks) or via connection to another network service (cellular service) as well as all portable and cloud storage devices.

Overview

The Information Services and Academic Computing Technology (IS/ACT) departments strive to provide the best customer service possible to all members of the College Community. Information Services and Academic Computing Technology (IS/ACT) departments have responsibility for specifying requirements for mobile computing devices used at NOCCCD. IS/ACT's responsibility to manage this policy and the use of these devices assists NOCCCD in managing district risk and the impact such devices can have on the operation of our infrastructure or the information stored therein. It will also allow IS/ACT to properly support and maintain these devices. NOCCCD has established and approved vendors for all services we provide. It is up to the discretion of appropriate campus committees in consultation with IS/ACT to change vendors if at any time the service provided is no longer meeting the needs of the College/District.

Policy

Information and information systems are valuable assets of NOCCCD. We rely on our information and information resources to advance our mission. Additionally, we are responsible to our donors, employees, and most importantly to the students we serve to ensure the integrity, confidentiality, and availability of

our information and information resources. To fulfill this responsibility NOCCCD has identified the following:

Cellular Phones/Cellular Data Plans

The use, purchase and replacement of cell phones are governed by Board Policy/Administrative Procedure 6450 the “Wireless or Cellular Telephone Use” policy.

Smart phones

A Smart phone includes network connectivity capabilities. The network connectivity capabilities range from connectivity to a Local Area Network (enterprise network) to internet connectivity through a service provider’s network. Phone devices used solely for work are purchased centrally through IS/ACT and are governed by Board Policy 6450 and Administrative Regulation 6450.

Laptops

In NOCCCD’s context, a laptop functions as a replacement for a desktop computer which provides the added functionality of wireless networking capability for increased connectivity and greater mobility. For laptops purchased through district purchasing the following requirements need to be met to connect with the network:

1. If a laptop is requested by an employee, the immediate management supervisor must decide if it is required for the position in his/her area. A justification is required to support the request and the accessories needed.
2. The dean/manager will be responsible for insuring that the laptop is properly inventoried and distributed.
3. Within a work area, laptops may be purchased and used as a “pool” of laptops to be signed out by staff for individual needs and controlled by the manager of the work area.
4. If laptops are assigned to an individual, the following conditions may apply:
    a. The associated desk top computer may be reassigned.
    b. The laptop should include a bag and as appropriate a cable lock.
    c. Auxiliary components if necessary must be funded by the requesting organization.
5. Installation of operating system, software and devices.
    a. Only properly licensed software is permitted to be installed on district owned equipment.
    b. IS/ACT in conjunction with the department that will be using the equipment will come up with a “Golden Image” that combines operating system and user applications. Exceptions to this are agreed to in advance by the department and ACT/IS.
    c. IS/ACT will provide software and license keys for software that is either purchased under a campus or district wide agreement.
    d. IS/ACT will provide support for operating systems and software installed in item “C”.
    e. IS/ACT can work with the department to install additional software that is purchased by the campus or district that is not covered by a campus or district agreement on a case by case basis.
    f. IS/ACT can attempt to provided support for software in item “E” but the group using the software is ultimately responsible for their own support.
    g. Users are not permitted without prior approval from IS/ACT to make changes to antivirus or firewall settings.
    h. IS/ACT does not support software without prior agreement.
    i. Third party applications or hardware that interferes with computer or enterprise network operations will need to be removed from the device that are installed or attached too.
    j. IS/ACT is not responsible for user’s personal software or data if it is determined the system must be reimaged to the “Golden Image”.
    k. Users are strongly encouraged to take advantage of enterprise network storage; either departmental shared or their personal home folder.

Tablet Devices

These devices typically function as a personal organizer, fax sender, reader and personal computer that incorporates handwriting recognition using touch screens, small keyboards, and/or voice recognition features. All devices such as these to be used solely for work purposes are to be purchased centrally through IS/ACT. Personally owned devices are allowed to connect to the campus wireless network if the following requirements are met:

1. Valid login credentials are presented to use district applications; no login is required if using Internet only
2. No printing will be performed except where the specific service is offered
3. No wireless to wireless activity will be performed (peer to peer).

Flash Drives, Portable Media and Cloud Storage

These devices/services can be used on computers and on the network provided by the district if they meet the following criteria:

1. Users present devices for use which are virus free
2. Users' password protect and use encryption if any data is of a confidential or personal nature.
3. Users' read terms and conditions of the provider and insure that data will not be shared without notification.

Selection and Purchase of Mobile Computing Hardware and Software

Standards for Mobile Computing Devices will be reviewed by the Technical Advisory Committee with attention given to cost, instructional functionality, business functionality, service availability, software compatibility, supportability, and security. These standards may specify models, vendors, related service providers, and software packages used with these devices.

Usage and Security of General Data

Given that Mobile Computing Devices may be storing and transferring confidential NOCCCD data while connected to the internet, all Federal and State Laws and Regulations and all NOCCCD Policies (Acceptable Use, Email, Data Security, etc.) are applicable and will be enforced. Mobile users must password protect access to stored information and take precautions to ensure the device is not lost or stolen. In addition, all data stored on mobile computing devices should be backed up regularly by the user to a location provided by IS/ACT for that purpose.

Some mobile computing devices have the ability to act as a modem allowing desktop or laptop computers to connect to the service provider permitting access to the internet. The IS/ACT Support Desk should be contacted before attempting this capability.

Support

Support for district-owned Mobile Computing Devices will be coordinated through the IS/ACT Help Desk. As some Mobile Computing Device functions require support from outside service providers (e.g. Verizon Wireless) the user will be responsible for working directly with outside vendors.

Network Access and Support

Authorized Cell Phone and Smart Phone users will be allowed to access any NOCCCD network directly through the Wi-Fi network, which may require authentication through a web browser.

Department Responsibility

Once an employee's employment with the College has been terminated, the immediate management supervisor is to immediately notify the IS/ACT Support Desk so that the service can be suspended if necessary. It is also the immediate management supervisor's responsibility to obtain all Mobile Computing Devices that are the property of the College before the employee physically leaves the College. If another employee (replacement employee) will take over the device/service, the immediate management supervisor must notify the IS/ACT Support Desk so that they can change the name of the user on the equipment and service plan and ensure the device and service is functioning properly.

Loss or Theft of Devices

Upon the loss or theft of a mobile computing device the employee must notify their immediate management supervisor. If required, the employee must file a report with Campus Safety and forward a copy of the report to the IS/ACT Support Desk. Upon receipt of the loss/theft report, IS/ACT will activate a process to wipe the data (if available) and user profile from the mobile computing device. The execution of this process will help ensure that private and confidential data that might be stored on the device will not be accessed and used inappropriately. If an employee should lose or damage a Mobile Computing Device, or if the department fails to collect the device from the employee upon separation from NOCCCD, the department will be responsible for the full payment to repair or replace the device.

Approved by the Technical Advisory Committee, November 15, 2011

Approved by District Planning Council/Chancellor's Cabinet, January 23, 2012

Reaffirmed by Technical Advisory Committee, February 26, 2013