CEHD Computing Security and Service Policy

This document is written in support of the following University policies:

- 1-14: Policy for Responsible Computing at the University of Delaware
- 1-15: Information Security Policy
- 1-18: Electronic Mail Management and Retention Policy
- 1-19: Employees' Use of E-Communications Policy
- 1-20: Policy for Wireless Computing at the University of Delaware
- 1-22: Personal Non-Public Information (PNPI) Policy

It also is written in support of best practices for computer and information security at www1.udel.edu/security.

Support Requests

The Office of Educational Technology (OET) provides device and network support to CEHD faculty and staff. This support includes technology consultation, configuring computers, malware detection, installation of virus protection software, automatic operating system and software updates, the installation of operating systems and productivity tools, diagnosis of printing problems, hardware and software recommendations, website development and support, and printer installation.

To request support for University-owned devices, write to oet-help@udel.edu, use the web form at www.oet.udel.edu/technical-support-request, or call (302) 831-8162.

Clients who request service on mobile devices (e.g., laptops, tablets, and phones) must bring them to OET's main office in 103 Willard Hall Education Building. For personally-owned and university-owned devices, OET can configure access to the OET network share, virtual private network (VPN), two-factor authentication (2FA), Multi Factor Authentication (MFA) and email. Cost for OET staff time to configure these items will be charged to the employee's unit. Because of the volume of calls and scheduled appointments, technicians cannot respond immediately to unscheduled requests for support, except in cases of emergency.

The Office of Educational Technology operates as a cost center and charges hourly for staff time based on services performed. These services include the following:

- Technical and desktop support
- Systems management (e.g., account creation, removal, permission assignments, folder creation)

- Technology consultation and web and database development

Rates are reviewed annually, in consultation with the University's controller's office and CEHD's business officer. For current rates, contact OET.

Computer, Network and Information Security Procedures:

- All CEHD equipment (University-owned) must be configured by OET immediately after it is purchased, to ensure that it is securely and properly configured. It is the responsibility of the unit to notify OET when equipment has been ordered and received.
- All equipment, including printers and mobile devices, must have password protection enabled. Passwords must not be blank.
- By default, OET will create standard user accounts on laptops and desktops. Supervisors may request elevated access privileges for a limited number of staff per unit, so that software approved by OET may be installed on unit devices by these staff.
- All CEHD (University-owned) equipment must have the following programs installed:
    - KACE (laptop or desktop)
    - Jamf (OS or iOS device)
    - University-recommended virus protection (currently McAfee for desktops and laptops).
        - Devices used to access financial, research and student data also have CylancePROTECT (security software) installed.
- Any device that is assigned to another employee must be visited by OET at the time of these changes, so that OET staff can clean the device of any previous data.

Data Security Recommendations

All CEHD faculty and staff have the obligation to protect University resources and data. Data protection measures include not sharing your passwords, locking your computer when you are away from it, safeguarding personally identifiable information (PII), and disposing of computers properly. To safeguard your data, especially in public areas, lock your computer session, when stepping away from the computer.

It is recommended that all CEHD staff complete data security training offered by Information Technologies through Secure UD training.

Passwords

Passwords are considered confidential information and should not be shared or written down. Strong passwords (12 or more characters) are used for your OET and University network accounts. If you need to share a password-protected computing resource with another staff member, contact OET for assistance.

Under no circumstances should staff and faculty share an individual's login and password. In certain circumstances, anonymous logins on the OET network are created and associated with specific computers.

Personally Identifiable Information (PII)

Personally identifiable information (PII) should not be kept on device hard drives or removable media such as DVDs and USB flash drives. Examples of PII include Social Security Numbers, credit card numbers, and grades associated with other identifiable information such as names. If absolutely necessary, this information should be encrypted and stored on a secure OET network drive and OET should be consulted regarding best practices for this information. For encryption solutions, contact oet-help@udel.edu.

The unit, and not OET, is responsible for ensuring that PII is not saved on local hard drives or in unencrypted formats on network storage space, and that all devices, whether or not they are used to handle sensitive information, are regularly updated and protected against attack and infection. See University Information Security Policy (1-15) and Personal Non-Public Information (PNPI) Policy (1-22).

Computer Inventory

The Office of Educational Technology will provide a computer inventory for each unit, if requested by the unit. This document will list all devices that have KACE (software that inventories devices and auto updates non-Microsoft products) and Jamf (software that inventories and pushes updates to Mac OS and iOS devices) installed. It is the responsibility of the unit to notify OET of any inventory changes, so that OET may remove devices from inventory. In addition, OET will record or verify in our service queue and in KACE and/or Jamf available equipment information, such as serial number and computer name, when we work on support requests.

File Storage and Retention
To prevent data loss, work files should not be stored on the physical hard drives of individual devices.

Backups of data saved on OET file servers are performed as outlined in the CEHD File Storage, Backup, and Retention Policy (PDF).

Specific guidelines regarding mail retention are outlined in University Electronic Mail Management and Retention Policy (1-18) and Employees' Use of E-Communication Policy (1-19).

OET User Accounts
Every faculty member, full- or part-time staff member, and graduate student in CEHD may receive an OET user account and file storage on OET's servers. Addition and deletion of faculty, staff and students on OET's network is not automatic. Units need to notify OET when individuals join CEHD and when they leave. In addition, OET will contact each unit at the beginning of the fall and spring semesters to verify if current accounts should remain active.

Computer Configurations
The currently supported operating systems within CEHD are Windows 10, Windows 8, and Windows 7 and for MacOS 10.11 or later. All CEHD computers must have current virus protection and current operating system updates applied, in support of the Policy for Responsible Computing at the University of Delaware (1-14). To protect the intellectual property of the College, each computer that contacts OET servers must have McAfee Virus Protection, KACE and Jamf (iOS and OS devices) installed. Computers may also be required to have CylancePROTECT security software installed, if deemed necessary. All Macintosh computers and iPads must have Jamf remote management profiles installed. In addition, Windows computers that are members of the OET domain have operating system updates pushed to them through Kace and Windows Server Update Services (WSUS).

Technology Recommendations/Purchases
Contact OET before purchasing any technology (e.g., software, hardware, phones, or printers). In addition, contact OET to arrange for network circuit testing, wireless strength evaluations, and wireless access point recommendations and quotes. This will help insure that CEHD devices have the required software and hardware to access University and OET network resources safely and securely, for warranty support, and for increased efficiency in computer configurations. In

addition, purchases through University-recommended vendors may qualify for discounts.

Anyone who purchases iOS and OS devices through the University Bookstore, will need to notify the Bookstore that the devices should be on the OET-dep. This is the device enrollment program for Jamf that allows us to push apps and updates to iOS and OS devices.

Units may elect to send mobile device purchases (e.g., laptops and iPads) directly to OET for set up. Units should notify OET when to expect the shipment, if they choose this option. Otherwise, units may bring mobile devices directly to our office for set up.

Except in the instance of computer refreshment (see the CEHD computer refreshment policy), OET cannot purchase computing equipment for units.

For home purchase recommendations, contact Information Technologies (IT), consult@udel.edu, (302) 831-6000.

Wireless Devices

In support of the Policy for Wireless Computing at the University of Delaware (1-20), wireless access points must be configured by University Network and Systems Services (NSS) or OET staff. In addition, wireless printers, while supported at the University, will require additional setup and configuration. For consistent connectivity, it is recommended that printers connect via an Ethernet cable to the University's network or directly to a device through a USB cable.

Moving Computers

The Office of Educational Technology does not move computing equipment. If you need a computer moved, contact University movers to move it to your new location. Before equipment is moved, contact OET to schedule an appointment to configure equipment in its new location.

Disposal of Computing Equipment

If you plan to dispose of computing equipment (e.g., tablets, laptops, desktops, hard drives), contact OET. An OET technician will record the device's name, remove it from our inventory systems, and wipe the device of data, using specialized software, to insure that your data is not compromised and is completely erased. Do not discard computers that have not been wiped by OET; doing so creates a security risk for you and your unit.

Once your computer is erased, contact University movers to deliver it to UD Surplus, or you may take it to UD Surplus yourself.

If a computer hard drive malfunctions and cannot be erased, complete a request for services form to have the hard drive destroyed. This service is free and performed by Information Technologies. You will need to deliver the hard drive to the computing center on campus, or OET can do this for you. If a computer hard drive malfunctions and is on warranty, it is highly recommended that the unit purchase the malfunctioning hard drive to promote data security, rather than return it to the manufacturer.

Technology-Related Exit Tasks

One week before a CEHD employee leaves a position, the unit head or other designee of that unit must contact OET to schedule the individual's email migration, if necessary, and reformatting of devices.

Employees are required to return all University-owned devices or property to their supervisor or his or her designee on or before their last day of work. The employee's supervisor is responsible for ensuring that all devices are wiped of all previous employee data and redeployed within the College, if still usable, or sent to Surplus. If devices are sent to Surplus, they must be wiped of all data by OET. Email oet-help@udel.edu with the name of the employee, date of termination and a list of the devices collected.

The Office of Educational Technology is notified monthly of terminations by CEHD's human resources hub. Upon receiving this notice, or as requested by CEHD's Human Resources Hub or the employee's supervisor, access to OET servers is removed the business workday following the termination date, the same business workday (i.e., if requested immediately), or on another requested date.

Before an employee leaves, the supervisor should review and/or plan to terminate the employee's access to the following. The supervisor should contact OET, if he or she has questions or needs assistance in requesting or changing permissions on these services:

- Public Calendars – Exchange and Google

- Shared mailboxes
- Other email distribution lists
- Google shared documents or One Drive shared documents
- Folders on OET shared drive that should be shared with others in the unit
- Personal UD email account – An employee is entitled to keep an email account active, if he or she is a current student, a January 2011 UD graduate or later, or a retiree.
- Restrict or remove access from websites
- Security codes on alarm panels
- Passwords on social media and any other public accounts
- Voicemail - Contact Telephone Services

In addition, the following items should be returned to the unit supervisor:
- Any CEHD-issued technology, including hardware and software, USB or flash drives, phones, and iPads
- Keys

Purchasing Devices upon Termination
Employees who leave CEHD may seek approval to purchase the computing device they use for the current fair market value. The employee must contact his or her immediate supervisor and the CEHD business officer for approval. If the purchase is approved by both, OET will determine in consultation with CEHD's business officer, a fair price for the device by reviewing devices with the same or similar components using online websites, including, but not limited to Amazon, Ebay, and Sage BlueBook. If the price is accepted by the employee and the unit, the employee may purchase the device from his or her unit. Prior to the sale, contact OET to remove all UD-licensed software that only is available to current UD employees.

Children's Campus Technology
In accordance with the Children's Internet Protection Act (CIPA), devices used by students on CEHD's children's campus must use a filter to prevent student access to inappropriate content. Information Technologies currently provides and configures this filter. Wireless devices used by students must access the Eduroam network with a specific user account. Passwords to this user account are changed approximately every six months and applied to devices. Wired devices are restricted by IP range. The Office of Educational Technology configures devices, records IPs, and works with IT to allow or disallow sites, upon request of the children's campus staff.

Parents and students at The College School (TCS) must agree to the terms of an acceptable use policy (AUP) and Google service guidelines so that the students may use available technology. The AUP is developed by TCS. Google service guidelines are developed by TCS, in association with OET.

Home Devices

In addition to support for University-owned computers, OET offers home computer support at our current hourly technical support fee. Clients must sign a waiver for service on home computers for each support request and are responsible for paying the fee.