

## **HSCDP INFORMATION TECHNOLOGY PROCEDURES & POLICY**

*[Items not reflected in current NCO Tech Policies are marked in Italic. It is not the imperative of this document to offer an alternative to NCOs tech policy, but to reinforce and in some instances further define policy and procedure and/or offer additional guidelines for HSCDP personnel. This document is an agreement to be entered into at the time of a new hire and is to be adhered to in conjunction with the NCO Electronic Communications Policy found in Section XIII of the NCO Policies.]*

In an effort to ensure that NCOHSCDP staff is informed about all information systems in our program, and to create a standard around the usage and privacy concepts of electronic mail, the Internet system and the computer network in general, NCOHSCDP has instituted the following Information Services Policy & Procedures Agreement.

NCOHSCDP has installed electronic mail (e-mail), VOICE-Mail and use of the Internet via its computer network to facilitate work-related communication. While NCOHSCDP respects the individual privacy of its staff a staff member cannot expect privacy rights to relate to work-related conduct or the use of NCOHSCDP owned equipment or supplies.

Accordingly, staff should note that the contents of messages on these systems are not entirely private. All information contained within the system is NCOHSCDP property. While it is not the policy of NCOHSCDP to routinely monitor or access a staff member's files, NCOHSCDP does retain the right to periodic unannounced inspections of its systems, for work purposes, at its sole discretion.

### **GENERAL POLICY AND GUIDELINES**

NCOHSCDP adopts a relatively good-faith policy of computer use. We don't have the resources to monitor daily network activity, document use, E-mail, web access, or much of our daily electronic activity. However, we reserve the right to enforce guidelines that haven't been followed and admonish repeat offenders. The need for a policy arises in part from the need to provide you with a consistent, stable, secure working environment through the establishment of computer hardware, software and network rules of conduct.

- Unauthorized use of other employees' passwords to gain access to sensitive or personal data is prohibited.
- Hardware and software allocations and access rights are determined by the IS department based on the agency business to be performed by that person or at that workstation. Rights and allocations may be changed at any time.
- Hardware and software donated to the agency become the sole property of NCOHSCDP and may be allocated according to agency needs (e.g., given to another user, sold, stripped for parts).
- All information created or stored on NCOHSCDP equipment or using NCOHSCDP accounts, is the property of the NCOHSCDP. This information may be accessed at any time by your supervisor or the IS department.
- All NCOHSCDP information stored on personal computers may be subject to access and removal by your supervisor or the IS Department
- *NCOHSCDP is not responsible for hardware or software brought from home, including damage, theft, viruses, data loss, and equipment failure.*

- *Unauthorized installation and/or download of software (all installations must have prior I.S. Manager approval) is prohibited.*
- *If your personal software causes your computer to be unusable, IS will remove it from the computer and you will no longer be allowed to use the software.*

## **E-MAIL USE & MAINTENANCE**

### Personal Use

NCOHSCDP staff are encouraged to send personal e-mail and conduct similar activities on their own time whenever possible. However, the occasional personal use of e-mail and other shared information systems during working hours is permitted within reasonable limits.

Personal messages will be treated the same as other messages in the system, which may or may not be archived from time to time and therefore subject to retrieval even after the user is thought to have deleted them.

*Users are reminded that with each Internet site visit and e-mail transmittal, NCOHSCDP's name is represented. Usage and messages must be accurate, appropriate, and should not subject NCOHSCDP to potential liability.*

*NCOHSCDP staff must keep secure passwords for their e-mail, known only to themselves at any time. However, the IS Department retains the ability to delete a staff member's password for any reason, including resetting the password if forgotten, or to check an account's mail if necessary (i.e., an attachment is disrupting the mail server while a staff member is on vacation, so it needs to be deleted from the mail server).*

Additionally, NCOHSCDP equipment may not be used to access or obtain or download any material that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale, including any message or graphic that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religion, ethnicity, physical or mental disability, political affiliation, color, marital status, gender identity or any other characteristic protected by federal or state law or local ordinance. Examples of offensive behavior include, but are not limited to:

- Personal attacks
- Offensive or obscene messages and or graphics
- Gossip, including personal messages about the sender or others
- Anything that may be construed as harassment or offensive to others.

### Bounced Mail

*If you receive a "bounced" message that the IS MGR. has forwarded to you, especially if it's with someone with whom you regularly communicate, please write the original author of the mail and let them know your correct E-mail address.*

### Attachments

#### *Receiving:*

- *E-mail attachments from unknown senders should be deleted without opening. If the attachment seems suspicious, notify the IS Department. Viruses are often spread by enclosing them in E-mail attachments that look legitimate.*
- *E-mail attachments from known senders should be scanned for viruses. Do not disable the automatic scanning that takes place on your machine. If you notice that no automatic scanning takes place, notify the IS department.*

#### *Sending:*

- *Attachments are not to exceed 1.5 M.B., or ~1500K. Attachments larger than this are likely to crash your E-mail client and/or cause problems with the mail server.*
- *If you know you're going to have to send a large file in advance, make arrangements with the IS Department to send the file. They can be split into multiple parts to send in separate e-mails. Once you're done, please delete the files from your Sent Mail folder to reduce the amount of space taken up in your mail client.*

### Storage, Filing and Maintenance

*Once you receive an e-mail and read it, if you want to keep it, please file it in an appropriate folder. If you do not know how to set up folders within Outlook, contact the IS Dept. Do not keep in excess of 300 e-mails in your In Box at any time. The more mail you store in you In-Box, the heavier a burden it is on the mail server and the network. If you receive e-mails with large attachments (large being 512K and up), please download the attachments and store them on you hard drive and delete the e-mail that sent the attachment.*

*Empty your "Recycle Bin". Delete sent mail in excess of 500 e-mails or once a month, whichever comes first.*

### Vacation Use

*If you are going on vacation but still wish to receive e-mail, make a request 1 week in advance to the IS Department including the e-mail account you'd like mail forwarded to, the starting and ending dates of the forward (the length of your vacation). However, this practice is discouraged on the principle that checking work related e-mail on your vacation is not a vacation.*

### Mailing Lists (Listservs)

*A mailing list is anything that you subscribe or were subscribed to by sending an E-mail with the content or subject heading "Subscribe person@whatever.org"*

*Inform the IS Department of any electronic mailing lists that you have subscribed to. If you'd like to subscribe to a work-related list but don't know how, fill out a request and you'll get training. The IS MGR. will establish a list-management filing system so that list mail does not stay in your In-Box.*

*If you would like a group account to be created (such as program-specific mailing lists or staff mailing lists), please consult the IS Mgr. We can create these, but it will take advance notice.*

### Establishing accounts

*See "Staffing Issues"*

### Terminating Accounts

See "Staffing Issues"

### **OTHER INTERNET USE**

*Use of chat rooms, including downloading of proprietary chat client software, is prohibited both through the Web and AOL. In the event that staff would like to attend a work-related chat forum, contact the IS MGR. with the date of the forum and the location. Help accessing forums is available as necessary.*

*Use of chat-based clients (i.e. Netscape, Yahoo, and AOL Instant Messengers) should be limited to personal time and reasonable use, like e-mail and SHOULD NOT start up with your computer's system startup. The IS Department reserves the ability to uninstall these programs permanently without notification, as they are considered personal software by the IS department. If it causes networking problems, it will be uninstalled and staff will be instructed not to install it again.*

*Installation and use of AOL client software on staff computers is prohibited. Oftentimes, AOL's networking software disables and/or deletes NCOHSCDP networking setup, preventing network security and virus protection from working properly. If you have a legitimate, work-related reason for using AOL, submit it in writing to the IS department.*

*NOTE: AOL-based E-mail can be checked from you web browser.*

*Staff should not download installable/executable files without authorization of supervisor and/or the IS Department. (This doesn't apply to basic information like Acrobat Reader, or PDF files; text files, or equally benign information.)*

*Staff should not use NCOHSCDP Internet accounts or titles for personal online purchasing.*

*No personal information should be given out; staff should identify themselves in any public or private forum with their name, title and the agency. Sites that require other information, such as address and phone number should be filled in using agency information.*

### **STANDARDIZATION**

*The NCOHSCDP operates on PC based hardware and Windows 2000 and Windows XP software. Any agency work that is not created on that platform is the responsibility of the staff creating it to translate to that platform.*

*Staff is responsible for using agency-standard software to do their jobs.*

*If our current software does not suffice, a software package may be ordered by request, with the understanding that the IS Department's ability to purchase software is dependant on budgetary constraints.*

### Personal Hardware/Software

- *You must have authorization prior to using your own hardware or software at NCOHSCDP, and it is generally discouraged.*
- *The IS Department will not maintain staffs' personal hardware/software without IS approval.*

### **DATABASE SECURITY**

*All NCOHSCDP databases contain sensitive and personal information about our clients, and staff. The integrity of its data is crucial to our confidential, fair and accurate reporting of information gathered from the communities we serve. Therefore, certain security and privacy precautions are necessary every time a database is used:*

- *DO NOT leave ChildPlus running while you're away from your computer. This leaves everyone's data open to the public.*
- *Check with IS before releasing the user-level password to any of the databases. Do not e-mail it to anyone; instead, tell them in person.*
- *Never e-mail confidential database reports.*
- *Never e-mail confidential documents without password protection.*

### **BACKUPS PROCEDURE**

*All staff are responsible for backing-up their data, either through storing files in their client named folder located on the desktop for Central Computers or on floppy disks at remote sites. Files from remote sites may also be sent via internal mail to IS staff for storage and backup.*

*Furthermore, any excessive backup time due to large **personal** files (unauthorized personal downloads such as movies, MP3s, and the like) will result in the immediate deletion of all such personal files and reported to the staff person's supervisor.*

*In the event that large downloads are work-related, notify the IS Department so make backup accommodations may be made.*

### **STAFFING ISSUES (Including Interns & Volunteers)**

***If a position requires computer skills, the supervisor should screen for those skills during the interview process.***

#### Establishing accounts

*Fill out a request form with two weeks advance notice to IS if you want an E-mail account established and the new staff trained on our system. We have a limited number of user licenses, so understand that it may take a bit of time to set it up. Also, if the request is for someone unfamiliar with E-mail, make sure to include that on the request so the new person can be trained properly and get a copy of these guidelines.*

#### Terminating Accounts

*NCOHSCDP allows for a "grace period" during which you can establish a new E-mail account and have mail forwarded to the new account. The forwarding will not exceed 30 days, and you must have your new account established prior to leaving NCOHSCDP. Alternately, the IS Department can establish an auto-reply redirecting mail to the*

*appropriate staff person and appraising people of your new E-mail address. Fill out a request form with two weeks advance notice to IS, if possible, include the final day of the staff person in the request. All mail is subject to deletion after the last work day of the staff member. Further, inform IS of any mailing lists the account was subscribed to so that they can be cancelled prior to termination of the account.*

#### Volunteer Use

- *Unless the role as a volunteer requires a specific machine, volunteers are not to use staff computers. They should only use computers designated for general use, such as the intern computers. Should a volunteer need a computer for themselves while working, please send a request to the IS MGR. with the same guidelines for hiring staff or an intern.*
- *Staff supervising volunteer use of computer equipment are responsible for reporting damage, viruses, data loss, and equipment failure in writing or E-mail to the IS Mgr.*
- *If a problem is the result of volunteer negligence or deliberate damage, supervising staff is responsible for assigning appropriate consequences and/or training.*
- *Supervising staff and or IS Mgr. are responsible for training volunteers in appropriate use of computer equipment and software and for monitoring their use; if a volunteer needs more training, please notify the IS department and we'll arrange a training for the volunteer and the supervising staff member.*

#### Working at home

- *If a staff member needs to establish e-mail or other programs for working at home, make a request in writing/E-mail to the IS department including the supervisor's approval, convenient dates/times for instructions. 1 week's notice is required.*
- *Any software provided for staff to use at home is the property of NCOHSCDP and may not be copied or used for non-agency business.*
- *Agency equipment that is loaned to staff is for work-related use only.*
- *The borrower is responsible for maintaining the equipment in good working order, and notifying the IS department of any problems.*
- *No other software may be installed, downloaded or otherwise transferred to agency computers.*

#### Training

*Any requests for staff training issues can be made directly to the IS Mgr. with 1 week's notice. Please consult with the IS department about all computer-related outside training, as we'll have suggestions and notice of upcoming trainings.*

### **FILE MANAGEMENT & SHARING**

*File sharing is vastly useful but can cause a burden on the networks and a security risk if done improperly. The following guidelines avoid these kinds of issues:*

- *All files should be stored in designated directories (i.e. documents in the Documents folder, applications in the Applications folder, etc.); network users should store files on the appropriate network drives to ensure backups and access from other stations if their computer is down.*

- *All disks brought from an outside source must be scanned for viruses; this is done manually using the Symantec Virus Protection application located under Start>Programs>Symantec Client Security.*

## **CONFIDENTIALITY**

Staff are responsible for protecting confidentiality of agency information by following all given guidelines including:

- *Keeping passwords confidential and changing them when directed*
- *Logging out of workstation and/or remote connection when not in use*
- *Not allowing any other staff or volunteer access to your workstation while you are working*
- *Locking offices when not present*
- *Reporting lost or stolen equipment or media*
- *Not copying agency information onto other media without authorization*
- *Having confidentiality agreements signed when sharing confidential information via disk, FAX or other electronic media between agencies*
- *Log off from network while away from workstation for Breaks, Lunches and Meetings, etc.*
- *Confidential Information such as client files are not to be sent via e-mail*

## **REQUESTS**

*Any formal requests that require one or more weeks' notice to the IS Department will need to use the appropriate request form.*

*All other requests can be e-mailed to the IS MGR., provided they fulfill at least some of the following:*

- *A complete description of the problem/request, including the symptoms of the problem or the requisition needed*
- *A relative deadline*

*Note: After reviewing this document in Orientation II, please sign and return "P909 IT Agreement.doc" to*

*Program Assistant/ Deputy Director Liaison for filing with employee file at North Coast Opportunities.*