Personnel Responsibilities in the Use of Information Technology Resources

Purpose: The intent of the following policy is to integrate technology as harmoniously as possible into the work place. It is intended to provide employees with consistent standards in regards to the use of computers, electronic mail, voice mail, and Internet access.

Policy: Use of CDS computers is restricted and must be consistent with CDS objectives/mission. Computer users must abide by copyright law, applicable local, state, and federal laws, and CDS guidelines. This policy applies to all employees/volunteers at all locations. All electronic and voice mail communications, including but not limited to stored information transmitted, received or archived in the CDS information system are the property of CDS. CDS reserves the right to access and utilize any information in its system as needed to protect and facilitate the legal and ethical interests of the organization.

Procedure and/or Process:

General Guidelines:

- Only personnel who have received supervisor approval and appropriate training are authorized to access CDS Information Technology (IT) resources.
- Authorized users will at all times ensure all IT security and confidentiality policies are followed.
- IT resources may not be used for commercial purposes, except for the business purposes of CDS.
- Staff sponsoring participant use of IT resources, whether on-site utilizing CDS computers or off-site (i.e. library), must maintain direct supervision of participants to ensure appropriate use of these resources.
- Regardless of the circumstances, individual passwords must never be shared or revealed to anyone outside of the Data Systems Department. Revealing a password to another party exposes the authorized user to responsibility for actions of another person.
- The safekeeping and functionality of mobile equipment that is assigned to an individual such as but not limited to cell phones and laptop computers are the responsibility of that individual. Expenses incurred due to misuse, personal use, or negligence will be the responsibility of the individual assigned.
- Staff who violates this policy may be subject to disciplinary action.
- Individual accounts are to be accessed only by the authorized users. Passwords are confidential and must be protected. Individual users will be held accountable for use of their account by others.

Computer Use:

- Do not change settings on any computer without the permission of the primary user or the supervisor.
- Staff are expected to exercise common courtesy and to respect the needs and sensitivities of coworkers/participants regarding computer use.

- Complaints about computer issues should be resolved directly by the parties involved whenever possible, but may be processed through CDS complaint procedures.

Software Use:
- Installation, upgrade, or removal of software is strictly prohibited and can only be performed by authorized Data Systems personnel.
- All users of commercial software products licensed to CDS are responsible for upholding the terms of the license agreements.

Internet Access:
- Staff may make reasonable personal use of internet at lunch and break time.
- Intentional use of Internet resources to access or process obscene material, inappropriate text or graphic files, or files dangerous to the integrity of the network is prohibited.
- Websites containing pornographic or offensive material should never be accessed from CDS computers.
- Staff are not to access any sites or services that may use excessive amounts of bandwidth (for example, video steaming sites) for other than work purposes.
- Staff are not to download files that may carry viruses.
- Staff are expected to use their common sense and ask questions if they are not sure about what they may access.
- Users must abide by the acceptable use policy of any accessed network.

E-Mail:
- E-mail communications should reflect the same level of professionalism expected of all other business communications. Some general guidelines are:
  - Use professional language, courtesy, and business etiquette.
  - Never send abusive, harassing, threatening, or ethnically oriented messages, even in jest.
  - Be careful when using sarcasm and humor. Without the personal interaction, your joke could be viewed as criticism.
  - Use common sense about what you say or send; you cannot control who will ultimately read it.
  - Never write anything to e-mail that you would not want to become public knowledge.
  - Review your message before you send it, a sentence that might be clear to someone talking to you face to face might come across quite differently without the tone of your voice or the facial expressions.
  - Think before you send e-mail to more than one person. Respect other employees' time. Do the additional people really need or want to see the message? Often an obligation is felt to respond or we want to express our own opinion. This then turns into a "chat" session.
  - E-mail to a participant should follow the same formality as a business letter. It should be treated as a formal document with proper business standards being followed. Spelling, grammar, and punctuation should be checked.

- The use of personal e-mail accounts to conduct CDS business, without prior supervisor approval, is strictly prohibited.
- All e-mail messages sent from computers must contain the CDS Confidentiality Statement.
- Participant information is confidential and every effort must be made to protect it when using e-mail functions. Refer to Policy P-1008 – Electronic Transmission of Protected Health Information.
- Before CDS staff release any internal CDS information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.
- Do not access another staff's mail files without permission.
- Misrepresenting, obscuring, suppressing, or replacing another user's identity on an e-mail system is forbidden.
- Transmission of unsolicited bulk e-mail spam, chain letters, pyramid schemes, and direct marketing pitches is strictly prohibited.
- Transmission of e-mails with sexual, ethnic, racial, and/or religious harassment content is strictly prohibited.
- Offensive electronic messages received must not be responded to. If they don't promptly stop, they must be reported to the immediate supervisor and CDS's Security Officer. (COO)
- Users must follow virus protection procedures for e-mail attachments (refer to Policy P-1066 – Virus Protection)
- E-mails are the property of CDS and their privacy is not guaranteed.
- E-mail may be used for personal use as long as it is used reasonably. However, this does not entitle staff to any expectation of privacy.

Voice Mail:

- Voice mail introductory messages should be professional and advise the caller of work related information.
- Voice mail messages left for others should be work related and should never contain derogatory, harassing, or unprofessional information.
- Voice mail must be protected with user or administrator set password.

Cell Phones:

- Cell phones are intended for business purpose and emergency use. Other use of cell phones should be kept to a minimum.
- Excessive personal calls, including roaming charges, or unauthorized use of telephone features may result in the need to provide reimbursement to the Fiscal Department upon receipt of the billing statement.