
Information Technology Usage Policy #174

General Provisions:

Computer Information Systems and the networks are an integral part of business at District 2 Public Health and the County Boards of Health that make up the District. They are an important resource to provide timely, efficient and cost effective data and communication services. All computers and computer related equipment are property of the County Boards of Health and/or the State.

Computers and networks are provided for employees who are affiliated with the County Boards of Health and District Office for the purpose of conducting Health Department business in support of the vision, mission and goals of the Health Department. This includes, but is not limited to, computers, network access, printers, modems, PDAs, and mobile telephones/radios. This same technology increases the risks of actions, deliberate or not, that are harmful in various ways, including: **1) interference with the rights of others, 2) violation of the law, 3) interference with the mission of District 2 Public Health, or 4) endangering the integrity of District 2 Public Health's information systems or network.**

All Users have a responsibility to use Health Department computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer resources, the Internet, or Protected Health Information may result in disciplinary action, including possible termination, and civil and/or criminal liability.

Purpose:

This policy is intended to protect the data on all District 2 Public Health's servers from security breaches to ensure that we meet HIPAA requirements and that our networks operate efficiently for the purposes of performing the business of the Health Department.

Administration:

The Information Technology Department (IT) is responsible for the day-to-day operations and administration of all networks and peripherals.

Employee Responsibilities:

1. Know and abide by all District 2 Public Health and County Boards of Health policies related to Information Technology; including security and confidentiality of business records.
2. Operate the equipment in a manner complying with all applicable District 2 Public Health Computer Usage Policies.

Intended Use of Equipment:

1. The use of Health Department equipment in political campaigns is forbidden.
2. Health Department equipment may not be used in connection with compensated outside work or for the benefit of organizations not related to the Health Department. State law restricts the use of tax payers purchased equipment for personal gain or benefit.
3. Computer users must obey all laws against private use of state property, divulging confidential patient records, copyright infringement, fraud, slander, libel, harassment, and obscenity.
4. Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone lines (modem).
5. Pyramid schemes and chain letters that ask for money or anything else of value are illegal.
6. Employees shall power off their computers at the end of the workday. A computer is considered off when the lights on the unit are off.
7. Employees shall logout when leaving their workstations.
8. Employees are prohibited from installing software regardless of the source. Exceptions must have prior approval from the IT Director. Approval can be acquired via email.
9. Employees are prohibited from allowing anyone that is not employed by the Health Department from using any Health Department computer equipment or peripherals.
10. Employees are responsible for maintaining backups of critical documents on CDs or floppy diskettes.
11. Employees may not add hardware or reconfigure any portion of the system without written approval from the IT Director.
12. Employees may not store personal files, of any type, on county / state owned computers. Personal files include, but not limited to, personal documents, photographs, videos, music files, etc.
13. Employees are responsible for reporting suspected criminal or administrative misconduct regarding misuse of County Board of Health technical resources to their Supervisor, Human Resource Representative, or the Security Officer.

Internet Usage:

1. Internet access is for Health Department business and may not be used for purposes that would violate any *Board of Health policy, Federal, State, or Local Law*.
2. Employees may use the Internet for occasional personal use to the extent that it does not interfere with work, or violate any *Board of Health policy, Federal, State, or Local Law*.
3. Excessive or inappropriate use or random web browsing unrelated to the business of the Health Department may result in loss of Internet access privileges and/or other disciplinary action.
4. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Information Technology (IT).
5. Employees may not use the Health Department's Internet connection to download entertainment software, screen savers, media player, or real player, etc. Additionally, you may not use the computer and/or network to display, store or send (via e-mail or any other form of electronic communication such as bulletin boards, chat rooms, UseNet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful. Furthermore, anyone receiving such materials should notify their supervisor immediately.
6. Do not click on Web pop-ups that promise to clean your computer or install needed patches.

Frivolous Use of the Internet is Prohibited. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Each office has a predetermined size/speed of circuit known as bandwidth to run their processes. Compare the bandwidth to a garden hose. When the hose is filled with water nothing else can get through. When the circuit is filled with data activity nothing else can get through, or it slows the data flow to almost nothing. It is important that employees utilize the existing circuit in the best interest of our business needs.

1. **Listening to music from the Internet is strictly prohibited. Viewing Streaming video or audio files on the Internet is strictly prohibited.** Disciplinary action will be taken.
2. **Participating in chat rooms or instant messaging is strictly prohibited.** Disciplinary action will be as taken.
3. **Accessing pornography or obscene materials via the Internet is strictly prohibited.** Accessing is defined by District 2 Public Health as displayed, generated, distributed, forwarded or stored using County Board of Health technology in any medium, such as, the Internet, software packages, email, storage devices, mobile telephones, computer hardware or peripherals.

Blocking Sites with Inappropriate Content: The County Board of Health has the right to utilize software that makes it possible to identify, track, and block access to Internet sites containing material deemed inappropriate for the workplace.

If an employee is found spending excessive time on personal use of these resources, this privilege may be revoked for that employee. If the offense is repeated it will be grounds for termination.

Electronic Mail (email):

1. While email is intended for official purposes, incidental and occasional personal use of the GroupWise email system is authorized. Users must exercise common sense and good judgment in the use of this resource.
2. Electronic mail should adhere to the same standards of conduct as any other form of mail. Respect others you contact electronically by avoiding distasteful, inflammatory, harassing or otherwise unacceptable comments.
3. Remember that you are responsible for all activity involving your email account. Keep your account secure and private. It is impossible for IT to guarantee total privacy. Under the Georgia Open Records Act it is possible that information, which is stored on our computer systems, including email, would be available for inspection by any member of the public.
4. The Electronic Communications Privacy Act (18 USC 2701-2709) and other wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.
5. **Transmission of Protected Health Information (PHI) via electronic mail is strictly prohibited *unless it has been de-identified*** (Reference: County Board of Health HIPAA Policy, Email Regarding Protected Health Information (PHI). Users should never open email attachments from outsiders, or use disks from non Health Department sources. If you receive an email that you think may be from a legitimate source but do not recognize the sender, contact IT immediately but do not forward the suspect email.

6. **You should never open email from unknown sources. Right click on the envelope and click on "Delete and Empty."**
7. Do not use personal email programs on County Board of Health workstations located in the facilities. These email programs bypass the safeguards that DHR/OIT and EMHD/IT have installed to protect the network from viruses. Personal email programs (Yahoo, AOL, Hotmail, etc.) may be loaded on laptops.

Passwords:

Passwords are an important aspect of computer security. Employees are responsible for creating, maintaining, and changing his/her password(s) in order to keep the networks of District 2 Public Health and beyond from being compromised.

Computer Viruses:

Computer viruses pose a serious threat to the security and integrity of Health Department computer systems, applications and data. While the potential for virus attack on standalone computers is considerable, there is a significantly more dangerous potential for virus attack on our networked computers due to the speed and ease with which viruses can spread across networks. District 2 Public Health has a responsibility to protect its resources against the threat of virus infection. All possible points of virus entry – the Internet, email, floppy disks, personal thumb/data drives, personal computers, gateways, servers, staff computers connected via modem – need to be considered and appropriate actions must be taken to counter the risks.

District 2 Public Health installs Symantec Anti-Virus software on all workstations and servers.

Virus Incident Reporting:

If the user believes their computer may be infected with a virus they should contact IT immediately. Please do not forward a suspect email to IT. The IT Department will assist in identifying any wide spread viruses. Users will not be blamed when reporting an incident and should be assured that they will receive assistance that is appropriate to the incident and their needs.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I, _____, have read

Please Print Employee's Full

Information Technology Usage Policy of District 2 Public Health and understand the procedures and guidelines I am required to follow to protect Health Department equipment and technical resources owned by the taxpayers. In cases of doubt, I bear the burden of responsibility to inquire concerning the permissibility of technology issues. Any questions should be directed to an IT staff member. This policy does not replace existing laws, regulations, agreements and contracts which currently apply to the identified resources of the Health Department. I understand the sanctions that may result in a policy violation. Any misuse or violation of the Information Technology Usage Policy will be judged in accordance with the published sanctions. I understand that if I observe, or have reported to me, a security breach or violation of this policy I should notify an IT staff member, my Supervisor, a Human Resource staff member, or the Security Officer immediately.

Employee Signature	Date
--------------------	------