IT RESOURCE ACCOUNTABLE USE

Policies & Procedures

DAVIS BEHAVIORAL HEALTH

SECTION:	IT Policies
PAGE:	1 of 4
SUBJECT:	IT Resource Accountable Use
EFFECTIVE DATE:	6/2010
REVISION DATE:	6/2013

PURPOSE

Davis Behavioral Health, Inc. (DBH) is the owner of hardware and software which provides current communications technologies and resources such as e-mail and the use of the Internet to support DBH service units and personnel in achieving their mission and goals. These resources are intended to assist in the efficient and effective use of Information Technologies (IT) in DBH daily operations, including collaboration and exchange of information within and between mental health agencies, associations and organizations, as well as government organizations and others. The resources also provide public access to public information.

This acceptable use policy is intended to establish general guidelines regarding the use of these technologies while maintaining the protection of DBH information and assets.

SCOPE

This policy applies to the entire DBH user community, including staff, volunteers, students and consumers, as well as Board Members, and any remote users authorized to access DBH electronic resources.

This policy applies to both information transmitted within the agency and to the sending and receiving of information through the Internet.

POLICY

It is the policy of DBH to assure that the use of DBH electronic resources are related to, or for the benefit of, Davis Behavioral Health and that Information Technologies are used productively. Also this policy is to inform DBH staff about confidentiality, privacy, and the acceptable use of DBH electronic resources. It is also the policy to assure that disruptions to DBH activities, because of inappropriate use of DBH Information Technologies are avoided and that IT resources may not be used for inappropriate purposes or in support of such activities. Inappropriate, as used in this policy, is defined as disruptive to the operation of DBH, as putting DBH in a position of legal liability, or as offensive to others, or as excessive use of IT for personal reasons not related to DBH purposes. **Anyone engaging in inappropriate/or prohibited use of Information Technologies may be subject to disciplinary actions which range from restricted use of some or all of these resources up to and including termination of employment.**

This policy is not meant to restrict the effective use of these resources, but to inform employees of the issues regarding their use.

PROCEDURES:

1.0 Electronic resources, such as telephone, voicemail, facsimile transmission, local and wide area computer networks, Internet/Intranet and electronic mail (e-mail), are to be used as an efficient means of communication.

1.1 As with all DBH assets, electronic resources are to be used in ways consistent with overall DBH policy. Generally, these resources are to be used for work related purposes. Occasional personal use of electronic resources is not prohibited by this policy. However, the expectation is that such correspondence will be subject to good judgment, common sense and courtesy, and the guidelines and considerations contained in this policy.

2.0 Davis Behavioral Health has the following Responsibilities and Disclaimers:

2.1 DBH must and will take reasonable steps to ensure its computing resources are free from destructive software, such as viruses. The DBH user community must share in that responsibility by using proper care to ensure the integrity of any electronic media they introduce.

2.2 DBH supports each individual's right to private communication, and will take reasonable steps to ensure the security of the network. However, since DBH owns the computer network system, normal computer operations as defined in this document, may reveal data. Also, DBH cannot guarantee the absolute privacy of electronic communications due to the potential for access to this type of communication.

3.0 The IT User has the following Responsibilities:

3.1 Access only personal files, data, protected accounts, and public information or files which you have been given authorized access to open.

3.2 Use the agency's IT resources efficiently and productively.

3.2.1 Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, or other IT resources.

3.3 It is the employee's responsibility to protect their individual passwords and for all activity performed under their individual login. Under no condition should employees give their passwords to another person. Passwords will be changed on a regular basis in accordance with existing password policies.

3.4 Maintain email inbox and archived communications. DBH strongly discourages the storage of large numbers of e-mail messages for several reasons. First, e-mail messages frequently contain confidential or personal information. It is desirable to limit the number, distribution, and availability of such messages to protect the information. Second, retention of messages fills large amounts of storage which greatly impacts the system efficiency. Therefore, employees should manage their e-mail messages by deleting those no longer needed.

4.0 Users of DBH IT Resources will avoid Unacceptable Use of those Resources

4.1 The following list includes, but is not limited to, examples of activities that represent inappropriate uses of IT and are considered to be prohibited uses of such resources unless authorized by DBH management.

4.1.1. Illegal Use. Defined as activities in violation of local, state, or federal laws. Such activities include any use of e-mail or other resources that is illegal or unethical and which would adversely affect DBH or put DBH in a position of legal liability. This includes copyright infringement, defined as the use of IT resources to copy and/or transmit any audio or video media, documents, software, or other information protected by the copyright laws.

4.1.2. Personal Commercial Use. Defined as any use to secure personal gain, advertise products, or participate in "for profit" personal activity. This includes activities such as "sport pools" and the selling of goods or services.

4.1.3. Sexually Explicit Material. Defined as any sexually explicit transmission regardless of whether it be visual, textual, or audio format; this includes pornography.

4.1.4. Religious or Political Lobbying. Defined as any use for religious or political solicitation or promotion.

4.1.5. Viruses. Defined as knowingly spreading computer viruses. Computer viruses are programs that can destroy valuable programs and data. To reduce the risk of spreading computer viruses, do not import or download files from unknown or disreputable sources. If employees obtain software or files from remote sources, proper procedures must be followed to check for viruses before use. If questions arise contact the LAN administrator.

4.1.6. Junk Mail. Defined as initiating or re-distributing frivolous materials such as "chain letters", advertisements, or unsolicited solicitations

4.1.7. Unauthorized Distribution of Confidential Administrative Information to Third Parties. Defined as unauthorized distribution of any proprietary financial or operational data that could jeopardize the operation of DBH or endanger its ability to be competitive in the marketplace. This includes budgets, bid responses for service contracts, personnel salary information, and sensitive confidential internal memoranda.

4.1.8. Obscene or Harassing messages. Defined as the transmission of obscene or harassing messages to any other individual whether within DBH or through the Internet. Employees should also be aware that such activities create a legal liability.

4.1.9. Confidential Consumer Information. Defined as transmitting confidential consumer information without proper authorization. This includes transmissions of such information to unauthorized organizations or persons, including DBH users who have no business reason for such information. (See HIPAA policies and procedures on DBH intranet)

4.1.10. Slander, Liable, and Defamation. Defined as the use of IT resources for transmission of information disparaging to others based on race, sex, age, or religion.

4.1.11. Broadcast Communications. Defined as sending the same message to large groups, including the use of DBH-All and other email groups. Mass distribution of messages in this manner uses large amounts of bandwidth on the e-mail system and has the potential to generate undesirable volumes of mail to be managed. **It should be used selectively and for compelling work-related reasons only**.

4.1.12. Unauthorized Equipment and Software. Defined as using non-DBH equipment or software on the DBH network or computer systems. This would include downloading music, movies, games, etc.

4.1.13. Social Networking. Defined as accessing websites such as Facebook, Myspace, Twitter, and UTube during work hours.

PRIVACY ISSUES AND LEGAL IMPLICATIONS

Users of both e-mail and the Internet should be aware that all transactions are logged by the computer system and, are available for recall. E-mail and Internet transactions may be accessed through the discovery process in the event of litigation.

By reading and signing this policy you agree you understand this policy and the procedures and will abide by the principles herein.

_____

Signature Date