

COMPUTER AND INTERNET USE

Applicability: This policy applies to all Oak Hill employees.

I. Oak Hill Property.

Oak Hill provides access to computers, email and the Internet for agency purposes and to increase employees' efficiency, productivity and accuracy. While some personal use of this technology is expected and anticipated, no personal use may unduly interfere with an employee's job duties and responsibilities.

No employee may use Oak Hill's computers, email or internet access for any illegal, unethical or inappropriate activities or purposes, including, but not limited to defamation; harassment; intimidation; solicitation; threats; coercion; the purchase or sale of illegal items; copyright infringement; "hacking"; profanity; racial, ethnic, sexual, religious or other derogatory slurs or epithets; insults; gambling; or accessing or distributing pornography. Violations shall be deemed a violation of Oak Hill's Standards of Conduct and Workplace Behavior policy and/or Sexual and Workplace Harassment Policy and may result in disciplinary action up to and including discharge.

Oak Hill encourages the business use of electronic communications (voice mail, e-mail, fax) and electronic data creation (documents, databases, and other electronic files) as a productivity tool. All messages and data created, sent or retrieved using Oak Hill computers, or using personal computers for Oak Hill business, are considered the property of Oak Hill, and not of the individuals who create, send or receive them. This includes messages and documents stored on the hard drives of any computer, cell phones, smart phones (i.e., data enabled), USB drives, external disks, or personal digital assistants (PDA) owned by either Oak Hill or the employee, and any work-related e-mails, documents, and databases stored on an employee's home computer, smart phone, or tablet that have been sent or received in the course of Oak Hill business. Oak Hill reserves the right to review this data at any time. When an employee terminates his/her tenure at Oak Hill, all electronic products remain the property of Oak Hill and may not be transferred or copied to the employee or any entity outside of Oak Hill.

No employee may tamper with any electronic records, documents or logs. Each employee is expected to comply with Oak Hill's Confidentiality and Privacy Policy regarding all applicable electronic records and documents.

Employees shall ensure that Oak Hill equipment is not damaged, altered or changed in any way that would prevent its use for agency purposes or create opportunities for its misuse for outside purposes. No employee may load, install, download or enable any Internet browser, install or download any new software or modify existing software without the approval of Oak Hill's Information Services Department. Storing personal documents, data and photographs on any Oak Hill computer or mobile device is

prohibited. No employee may engage in any behavior or activity that jeopardizes the security of Oak Hill's information systems.

II. Blocking Internet Access.

Oak Hill uses software to block access to certain Internet websites with subject matter that is inappropriate or irrelevant to the conduct of Oak Hill business. Occasionally this software may block a site for which an employee has a legitimate need for access for business-related purposes. In such cases, employees should contact the Help Desk for assistance.

The following uses of Oak Hill's computer system are prohibited and will be blocked as they impact the operation of the system:

- Downloading music;
- Using file-sharing systems; and
- Streaming video and audio, unless for a legitimate business purpose.

III. User Accountability for Security of Data.

To prevent unauthorized parties from obtaining access to electronic communications, users should choose passwords that are difficult to guess. Individual passwords must never be shared or revealed to anyone besides the authorized user. Users must not leave passwords on or near laptops or other mobile devices. To do otherwise exposes the authorized user to liability for actions taken by the other party using the password.

For security reasons, user passwords must be changed four times a year. The terminal login process will prompt you when it is time to select and register a new password.

Copying Oak Hill data onto USB (portable) drives or disk media must be done so with the express purpose to move the data to another Oak Hill machine or for temporary use in another location. Data on this media must be locked and secured (encrypted) separately from the laptop or portable device to insure its confidentiality. You are responsible for the care of the data being transported on portable media. This policy does not apply to disks or drives that contain video and/or data used for the express purpose to promote our development initiatives or programmatic purposes.

Employees whose laptop, storage device or data is lost or stolen must notify the HIPAA Privacy Officer and the Director of Information Technology immediately and report whether the device or data contained any information that may be considered a data breach under Oak Hill's HIPAA and HITECH policies.

Any employee who observes or becomes aware of any violation of this policy shall report the matter to the Director of Information Services.

Cross reference: Confidentiality and Privacy
Laptop Policy

Privacy Protection Policy
Protecting Documents and Data
Sexual and Other Forms of Harassment
Standards of Conduct/Workplace Behavior
Social Media

Originally published May 1, 2006
Revised June 12, 2008
Revision approved: March 30, 2011

Revisions to this policy are effective April 15, 2011