

USOE Official IT Policies and Procedures	
Policy: USOE Network Standards and Connection Policy	Page: 1 of 3
Subject:	Data Modified: 10/13/08
Purpose:	

(Definitions of *bold & italicized* terms are listed at the bottom.)

Two classes of computers may connect to the *USOE network*. Please note the restrictions that apply to each class.

1. Owned by the USOE.

This computer may be connected directly to the *USOE domain* via cable.

All USOE owned machines are purchased, installed, configured, and maintained according to *USOE hardware and software standards* by the USOE network administrators. Additional software may be installed only with the approval of the USOE network administrators.

Additional software may be installed only with the approval of the USOE network administrators. If the USOE owned computer is a notebook, it may also be used for *telecommuting*. It may be configured for *VPN* to access the *USOE domain* from the Internet or through the *USOE wireless network segment*.

Only USOE owned computers will be allowed to connect to the USOE domain, directly or indirectly through a VPN connection.

2. Privately owned and brought into the USOE by a business visitor.

A business visitor may access the Internet, but not the *USOE domain*. USOE has an open wireless system that visitors can connect to. To access the Wireless Internet, they must receive permission along with the current username, password, and instructions from a USOE employee in order to connect to the *USOE wireless network segment*. With these credentials, the business visitor is responsible for configuring, and establishing the wireless Internet connection. If the business visitor does not have a wireless network adapter, they may still connect to the Internet via cable and specially marked data jacks in conference rooms throughout the building.

The business visitor must be asked to assure their host they are using a *secure computer* and are willing to abide by the *Acceptable Use Policy*.

Note about PDAs (personal digital assistants). No PDA or other handheld device may, by itself, be directly connected to the USOE network, wirelessly or with cable. When

USOE Official IT Policies and Procedures	
Policy: USOE Network Standards and Connection Policy	Page: 2 of 3
Subject:	Data Modified: 10/13/08
Purpose:	

properly configured such devices may be used to synchronize with the host computer or download network files including those in Outlook, This is only permissible through a USOE owned or *telecommuting* computer by means of an attached cradle or Bluetooth wireless technology. **Violators of this policy may be subject to disciplinary action.**

USOE is not responsible for lost data or damage to any privately owned machine that is connected to *USOE wireless network segment* or the *USOE domain*.

Definitions

Acceptable Use Policy. All employees and business visitors, regardless of how they are connected to the USOE network are required to follow the USOE acceptable use policy. See: <http://www.usoe.k12.ut.us/hrm/acceptuse.htm> & <http://www.governor.utah.gov/lan/aup.htm>. Also note the acceptable use policy states:

Also, please note the acceptable use policy states that the use of resources for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc., or other uses that waste resources or disrupts performance, is prohibited.

This includes use of agency machines for streaming audio and video when not work-related. **Violations of the acceptable use policy may be grounds for termination.**

Telecommuting. USOE employees may telecommute with management approval. Telecommuters must use a USOE owned computer. If the telecommuter desires to connect to the *USOE domain* through the Internet and *VPN*, they must secure their own Internet connection. See <http://www.usoe.k12.ut.us/hrm/rules2002.pdf> for more information about telecommuting.

USOE domain. The USOE domain is the secure network of shared computers at the USOE. It is a subset of the more generally defined *USOE network*. The domain includes all servers and user computers, each connected to one or more of those servers. These machines are all behind a firewall and other security devices and software such as intrusion detection and filtering servers. When a user connects to the USOE domain from within the building by supplying a logon name and password they also receive Internet access. Business visitors are permitted to connect to the USOE wiring infrastructure and obtain Internet access without connecting to the USOE domain. Such use is permitted only through the *USOE wireless network segment*.

USOE Official IT Policies and Procedures	
Policy: USOE Network Standards and Connection Policy	Page: 3 of 3
Subject:	Data Modified: 10/13/08
Purpose:	

USOE hardware and software standards. In order to maximize usability, reliability, security, and efficiency of USOE information technology resources; the USOE has defined hardware and software standards. A summary of the current hardware/software standards include: a Dell desktop or notebook running Windows XP with the latest service packs and updates installed, and the latest Microsoft Office suite of productivity applications including the Outlook e-mail client. As part of the USOE standard setup features, these machines are all configured as **secured computers**. Other hardware and software standards exist in the USOE, but most involve network infrastructure and custom application development and deployments. Always check with network administrators before purchasing software or hardware to see if it is compatible with the USOE network, and if an agency license agreement (in the case of software) already exists. Installation of software for purely personal use is prohibited. All installed software must be for work related activities and must be owned by USOE.

USOE network. The USOE network is defined as the entire computer infrastructure within the USOE including all wiring, communication devices, routers, switches, servers, desktops and other connected computers. The **USOE domain** is a subset of this network.

USOE wireless network Segment. A secure wireless network segment is available for USOE staff and sponsored business visitors. This network provides access to the Internet and optionally to the USOE domain via VPN. In order to connect to the USOE for Internet and/or USOE domain access, the USOE employee or business visitor must first acquire the current credentials and configure the computer to recognize and connect to the USOE wireless network segment. For security reasons these credentials may change periodically. When this happens they will be distributed to all USOE employees who have a VPN account. Currently the USOE supports the IEEE 801.11b and 801.11g wireless protocols.

VPN (virtual private network). VPN allows those with USOE domain accounts to access the USOE network remotely or through the firewall. You must have a VPN account established by a USOE network administrator before you can access the domain using VPN. Only network administrators will be able to configure VPN access. If you need VPN access please contact the Help Desk.