EASTERN CONNECTICUT STATE UNIVERSITY
Information Technology Services
Management of Smart Devices Connecting to the University Network

Definition: A smart device is an electronic device that is cordless (unless while being charged), mobile (easily transportable), always connected (via WiFi, 3G, 4G etc.) and is capable of voice and video communication, data, internet browsing, "geo-location" (for search purposes) and that can operate to some extent autonomously. It is widely believed that these types of devices will outnumber any other forms of smart computing and communication in a very short time.

When connecting to the University network the device must meet certain standards to ensure the security and integrity of Eastern's technology infrastructure. All smart devices must be password protected when connecting to the University's network. Smart devices connected to the email server should never be left alone and the device should be set up to lock after one minute of inactivity. With all smart devices, the systems must be properly patched with the latest operating and security controls.

When connecting to the University network, staff and faculty will comply with the following standards.

1. You are responsible for safeguarding and controlling access to the device.
2. Smart device will be password enabled with a minimum of 4 characters.
3. The smart device will have a 1 minute security time out.
4. Theft or loss of a University owned smart device connected to the Exchange Server will be reported to ITS, Exchange Administrator or the Chief Information Officer, immediately. Staff must immediately change their password to protect the University network. If possible, the Exchange Administrator will remotely wipe out any data on the phone. Privately owned phones connected to the Exchange Server must also immediately reset their password. If possible have your wireless carrier disable the device.
5. When replacing or upgrading your smart device the old device's data must be wiped clean. On University owned devices, the Exchange Administrator can assist you in this process. Staff with privately owned devices should contact their provider for assistance if needed.
6. As with all portable devices no sensitive data or confidential information shall be housed or transmitted on a smart device.
7. Should you retire or leave employment of the University, access to the Exchange Server will be reviewed and granted on an exception basis by the Human Resources Department.

If you require assistance in using your smart phone, please don't hesitate contact ITS, Exchange Administrator (Fawng Li) 860-465-5382 or the Support Services Director (Kevin Gill) at 860-465-5793. By signing this document you are agreeing to abide by the procedures outlined above.

Device Holder Signature Date	Chief Information Officer Date
Printed Name	Stephen Nelson