

Wireless Access Policy

POLICY:

Authorized users of Darton College computer systems networks and data repositories may be permitted to use wireless technology to connect to those systems, networks or data repositories to conduct College related business only through authenticated and centrally managed access methods.

Rationale:

Increase in the availability of wireless technology and the ease of deployment has significantly increased the potential for unauthorized access to College information systems. Deployment of the Wireless system established a framework for authenticated access across the campus. Establishing policy centrally and configuration and management of access points by a central authority allow a minimum number of penetrations of the security of the network.

Standards & Procedures:

Standards:

Access Method. All access through wireless access points connected to the College network infrastructure (regardless of duration) will be authenticated using userid and password. Mobile access points will be permitted to operate only from network ports configured by the Office of Information Technology (OIT) for this purpose.

Configuration, Installation, and Management. All fixed wireless access points connecting to the College network infrastructure will be configured, installed and managed by OIT. Existing access points must, as a minimum, provide 802.11b service and be configurable to block broadcast of SSID.

Unauthorized Access Points. OIT will periodically check the campus for unauthorized fixed and mobile access points, immediately disable the network ports supporting those access points and advise the operating department of necessity to comply with this policy.

Procedures:

None