Board Adopted Policy	
Policy Title: **Public Wireless Access**	
Effective Date: 07/11/2012	Review Cycle: Three (3) Years
Board Approval Date: 07/11/2012	Review Date: 06/18/2015
Review Date: 06/19/2018	

I. Application: Authority wide

II. Intent: The Benzie Transportation Authority (Authority) provides free Internet access points in public meeting rooms within its administrative offices for users with portable computers or devices capable of receiving wireless signals. These access points will allow users to access the Internet from their laptop computers when sitting within range of the access points. The Authority is providing wireless connectivity in this facility and vehicles as a public service and offers no guarantees or representations that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of this wireless connection is entirely at the risk of the user, and the Authority is not responsible for any loss of any information that may arise from the use of the wireless connection, nor is the Authority responsible for any loss, injury, or damages resulting from the use of the wireless connection.

III. Procedure: As a public agency, the Authority has a management responsibility to establish an appropriate policy to administer use of the Internet and online services supported by the Authority. It is within this context that the Authority offers access to the Internet via the public wireless network.

All users are expected to use the Authority's wireless access in a legal and responsible manner, consistent with the public and informational purposes for which it is provided.

While using this wireless access, users should not violate federal, State or local laws, including:

1) The transmission or receiving of child pornography or harmful material. Access to or display of obscene language and sexually explicit graphics is not permitted.
2) Fraud – Users are prohibited from misrepresenting themselves as another user; attempting to modify or gain access to files, passwords, or data belonging to others; seeking unauthorized access to any computer system, or damaging or altering software components of any network or database

3) Downloading copyrighted material. U.S. copyright law (Title 17, U.S. Code) prohibits the unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use". Users may not copy or distribute electronic materials without the explicit permission of the copyright holder

By using this wireless access network at the Authority, the customer acknowledges that user is subject to, and agrees to abide by all laws, and all rules and regulations of the State of Michigan, and the federal government that is applicable to Internet use.

1) User will need a notebook/laptop computer or other device equipped with a wireless card that supports the Wi-Fi standard (IIEE 802.11b/802.11g).

2) The Authority assumes no responsibility for the safety of equipment; Users must keep their equipment with them at all times and may only use electrical outlets in public areas.

3) User will need a notebook/laptop computer or other device equipped with a wireless card that supports the Wi-Fi standard (IIEE 802.11b/802.11g).

4) The Authority assumes no responsibility for the safety of equipment; Users must keep their equipment with them at all times and may only use electrical outlets in public areas.

5) Authority staff will not provide technical assistance. The Authority assumes no responsibility for laptop configurations, security or changes to data files resulting from connection to the Authority's network and cannot guarantee that a user's hardware will work with the Authority’s wireless connection.

6) If a user has problems accessing the Internet over these connections, staff will not assist in making changes to the user's network settings or perform any troubleshooting on the user's own computer. Users should refer to their owner's manuals or other support services offered by their device manufacturer.

7) The Authority has tried to ensure wireless access is available in its public meeting rooms. However, users may encounter occasional "dead spots" where wireless reception may be limited or too many users are attempting to access from a particular access point. If you have trouble accessing the Internet or staying online, please move to a different location within the meeting rooms.

8) User will automatically be prompted to accept the terms of the BTA Public Wireless Access Policy prior to Wi-Fi access.

Security Considerations

Wireless access is by nature an insecure medium. As with most public wireless networks, any information being sent or received over the Authority's wireless network could potentially be intercepted by another wireless user. Cautious and informed wireless users should not transmit their credit card information, passwords and any other sensitive personal information while using any wireless "hot spot".

Anyone using the wireless network provided by the Authority is forewarned that there can be no expectation of privacy when using the wireless network, whether accessed from an external or internal site. Users assume all associated risks and agree to hold harmless the Authority, its directors, officers and employees for any personal information (e.g. credit card) that is compromised, or for any damage caused to users' hardware or software due to electric surges, security issues or consequences caused by viruses or hacking. All wireless access users should have up-to-date virus protection on their personal laptop computers or wireless devices.