BERS-Guest Wireless Internet Acceptable Use and Safety Policy

Guest Wi-Fi User Disclaimer

The BERS-Guest Wi-Fi (wireless) is an open unsecured internet connection provided to members and guests visiting BERS office. The BERS-Guest Wi-Fi connection is a free internet service provided to visiting members and guests by BERS. Access is completely at the discretion of BERS, and may be blocked, suspended, or terminated at any time for any reason including, but not limited to violation of this Policy, actions that may lead to liability for BERS, disruption of access to other users, networks or third-party, or violation of applicable laws or regulations. BERS may revise the terms of this Policy at any time. You must agree to the terms of this Policy each time you access the BERS-Guest Wi-Fi connection.

User Agreement:

The BERS-Guest Wi-Fi allows for visitors with mobile devices to connect to the Wi-Fi Internet. By clicking on the "Continue to the Internet" button you are connecting to the Wi-Fi network as a BERS-Guest and are agreeing to abide by this Policy, Department of Education (DOE) regulations policies and guidelines, and applicable law.

Wireless Internet access is, by nature, a non-secured connection method. Any information being sent or received over the BERS-Guest wireless network could be intercepted by another wireless user. Wireless users should not transmit their credit card information, passwords, and any other sensitive personal information while using the BERS-Guest Wi-Fi connection.

Users have no right to privacy while using BERS's Internet Systems. BERS reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law.

Limitation of Liability

BERS makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. BERS also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the Wi-Fi connection is understood to be the author's individual point of view and not that of BERS, DOE, the City of New York, or their respective officials or employees.

Terms and Conditions of Use:

Guests will need a notebook/laptop computer or other mobile device with a wireless card or connection that supports all current Wi-Fi standards. BERS assumes NO responsibility for the safety of the equipment used. By using the free BERS-Guest wireless internet service, you are agreeing to the disclaimer set forth above.

Prohibited Uses of BERS Internet Systems

Users may not engage in any of the activities prohibited by this policy when accessing BERS-Guest Wi-Fi.

Below is a non-exhaustive list of examples of prohibited behavior:

1. Causing harm to others, damage to their property or BERS property, such as:

    - Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, material posted on BERS web pages, or professional social media sites;
    - Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by BERS IT Department;
    - Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
    - Engaging in spamming;
    - Damaging computer equipment, files, data or BERS's Internet System in any way;
    - Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws;

2. Gaining or attempting to gain unauthorized access to BERS-Guest Wi-Fi or BERS Internet System, or to any third party's computer system, such as:

    - Malicious tampering, phishing or hacking activities;
    - Attempting to gain access to material that is blocked or filtered by BERS;
    - Disguising a user's identity;

3. Engaging in criminal or other unlawful activities.

4. Use of cross-platform instant messaging and Voice over IP services including, but not limited WhatsApp, Google Talk, Viber, Skype, Hangouts.

5. Use of streaming media and video-on-demand services including, but not limited to Hulu, Netflix, Amazon Video.