International Balkan University (IBU)
Student Wi-Fi Usage Policy

This policy outlines the rules and guidelines for student access and usage of the university's Wi-Fi network. The university aims to provide reliable internet access for educational and research purposes while ensuring security, appropriate usage, and network integrity.

This policy applies to all students who use the university's Wi-Fi network. It defines the conditions for accessing the network, acceptable internet use, and users' responsibilities.

1. **Wi-Fi Access**
    - **Active Directory Authentication**: Access to the student Wi-Fi network is restricted and managed through the university's Active Directory system. Each student must authenticate using their unique university-issued credentials (username and password).
    - **Login Credentials**: Students can find their Wi-Fi login credentials in their Hello! Dashboard, which is accessible through the university's online portal. These credentials must not be shared with others.
    - **Connection Limits**: Students may connect a limited number of personal devices to the Wi-Fi network. The IT department will determine the number of allowable devices.
2. **Restricted Internet Access**
    - **Educational Use**: The primary purpose of the student Wi-Fi network is to support educational activities such as accessing online course materials, conducting research, and participating in academic discussions.
    - **Content Filtering**: The university reserves the right to restrict access to specific websites and online content deemed inappropriate or non-educational. This includes but is not limited to, adult content, illegal file-sharing websites, gaming platforms, and social media sites during academic hours.
    - **Bandwidth Management**: The IT department will monitor and manage bandwidth usage to ensure equitable access to the Internet for all students. Bandwidth may be limited during peak hours to prioritize academic activities.
3. **Usage Monitoring and Privacy**
    - **Network Monitoring**: The IT department will monitor student Wi-Fi usage to ensure compliance with this policy. This includes tracking bandwidth usage, monitoring security threats, and enforcing content filtering rules.
    - **Privacy Considerations**: While the university respects students' privacy, internet usage on the university network is subject to monitoring. The university does not monitor personal data, but network activity related to inappropriate or unauthorized use may be investigated.
4. **Security and Data Protection**
    - **Secure Login**: Students must use secure login methods when accessing the Wi-Fi network. This includes using encrypted connections (e.g., HTTPS) when accessing

sensitive information online.

- **Personal Device Security**: Students ensure their devices have up-to-date antivirus software and are malware-free before connecting to the Wi-Fi network.
- **Prohibited Activities**: Students are prohibited from attempting to bypass network security controls, accessing unauthorized resources, or engaging in any activity that compromises the security of the university network.

5. **User Responsibilities**
    - **Compliance with Policies**: By using the university's Wi-Fi network, students agree to comply with this policy and other relevant university policies, including the Acceptable Use and Information Security policies.
    - **Respectful Use**: Students must use the network resources responsibly and refrain from activities that may disrupt the network, such as excessive downloading, streaming, or unauthorized use of network resources.
    - **Reporting Security Incidents**: Students must immediately report any security incidents, such as suspicious activity or compromised accounts, to the IT department.
6. **Support and Troubleshooting**
    - **Help Desk**: The IT department provides assistance to students experiencing issues connecting to or using the Wi-Fi network.
    - **Access Revocation**: The university reserves the right to revoke Wi-Fi access for students who violate this policy or pose a threat to network security. Repeat violations may result in disciplinary action.
7. **Enforcement and Disciplinary Action**
    - **Policy Violations**: Any violations of this policy may result in restricted network access, account suspension, or other disciplinary actions under the university's disciplinary procedures.
    - **Legal Consequences**: Engaging in illegal activities on the university's Wi-Fi network (e.g., copyright infringement, hacking, or distributing illegal content) may result in legal action as per applicable laws and regulations.
8. **Policy Review and Updates**
    - The IT department will review this policy annually and update it as necessary to reflect technological changes, university needs, or environmental regulations.