Terms of Use

The use of the wireless network implies that you have agreed to the following policies:

1. Network users will have WIFI access to the network established and governed by the school regarding network access. Network users are responsible for any and all activities that take place on said device.
2. Any transmission and/or distribution of material that violates any law is prohibited. For example, the use of intellectual property without the proper authorization, or the copying of programs or applications unless your license allows it.
3. It is prohibited to transmit and / or distribute any discriminatory, hostile, degrading, or intimidating material for any person or group of people, whether due to religion, gender, sexual orientation, race, age, disability, etc.
4. The transmission of illegal, abusive, or questionable material is prohibited.
5. The transmission of messages or information that infringes on a person's right to privacy.
6. Spam of any kind to any recipient is prohibited.
7. Using the school's wireless network for commercial purposes, personal advertisements, or promotions is prohibited, unless authorized by the school.

   Any network user who violates these policies will be subject to disciplinary sanction, in addition to any possible legal action that may be taken.

Consequences and Sanctions

Accidental or minor violations of these policies will be reported to area managers via email for discussion and educational purposes.

Serious violations, including repeated minor violations, may result in the suspension or deletion of your wireless network access account.

Process and Supervision of WiFi

- Before accessing the Institutional wireless network, each user must register their devices. This does not apply to public networks that will be left for visitors in certain sections (Employees who receive equipment assignments are previously registered).
- A maximum number of devices that can access the wireless network per section will be delimited.
- Appoint at least 3 user administrators to register and grant keys when necessary, distributed in critical sections (In this case, go to systems).
- Delimit the bandwidth by types of users stipulated by each section or following the recommendations of user administrators.

- Monitor the traffic of the most used applications, identifying if more bandwidth is needed than stipulated for users.
- Stipulate types of users based on the analysis of each section

Advantages
User control and access permissions.
Control of content by user.
Internet Broadband Control.
Lower Saturation.
Better fluidity of the internal network.
Greater security.
Managed networks can be improved.
Justified Use.
Compatibility with new technologies
Simple and intuitive interface.
Administration from the Cloud.

Disadvantages
Access times and configuration

Recommendations for Safe Internet Browsing

Take care of what you post on social networks (Users).
Activate privacy settings (Domain Administrators).
Safe browsing practice (User).
Check that your network connection is secure and authenticated
Domain administrators).
Be careful what you download. (Users)
Keep your antivirus updated. (Domain administrators and users)
Accept only known contacts. (Users)