PROVISIONS FOR THE USE OF THE WI-FI NETWORK

The Ersu of Sassari provides access to the internet for all students who have a bed in their residences.
The service, exclusively wireless, allows the mobility of terminals within the various residences (Via Coppino, Via Manzella, Via Rosello, Via Verona, Ex Brigata) using the same credentials provided by the Administration.

The first access to the wireless network will constitute a declaration of acknowledgment and total acceptance of these Provisions for the use of the wi-fi network.

1. General rules

Failure to comply with the Provisions will result in immediate measures that will be assessed according to the severity of the action taken and its recidivism with the consequent permanent deactivation of access rights.The activities carried out on the network will be kept track with the user's credentials. The Administration will not access such data which may, however, be made available to the judicial authorities if requested by these as a result of illegal activities or conduct.Finally, it is reiterated that all civil and criminal liability lies with the individual users of the network.In case of violation of these Provisions, the Administration will proceed to the formal recall of the user and, if necessary, make the related documentation available to the judicial authorities.

2. Access rights and credentials

Access to the service takes place through a special key which remains strictly personal and which can be associated with only one device. The key lasts for the entire academic year.The user is responsible for the diligent custody of their wireless network access credentials. Any irregular activity will be attributed, within the limits of the law, to the owner.These credentials, being uniquely associated with its owner, are strictly personal and therefore not transferable. Should they be transferred to others, the responsibility for the activities carried out by them on the network will in any case fall on the holder of the credentials.The user is obliged to immediately report any suspicion of break-in, accident, abuse or security breach;Ersu di Sassari assumes no responsibility in the event of improper use of login credentials.The use of access credentials to IT services will be recorded in special files (Log) for the uses permitted by law and by these provisions.If the user suspects that their credentials have been compromised, they must promptly notify the Accommodation Sector.The infrastructures and services are owned by Ersu of Sassari. The same administration may interrupt, prohibit, block access and the service, even to individual users, without notice and at any time.To allow everyone to use the service, each user is allowed to use only one personal device of their choice at a time (PC, tablet, smartphone, etc.).

3. Rules of conduct

The user undertakes to comply with the rules of conduct indicated below:

a. Use only the resources for which the service is enabled: it is possible to freely access the Internet but the Administration may at any time decide to inhibit, at its discretion, the services it deems harmful for optimal use of the available bandwidth (programs for file exchange, chat, etc.). The network should be used mainly for educational purposes
b. Do not attempt network scanning actions or security attacks as they are expressly prohibited by law. It should be noted that for events such as those mentioned above, it is possible to identify the device and account that originated them;
c. Never use the Organization's network to exchange illegal material: the exchange of copyrighted material (e.g. MP3, DivX or DVD films, commercial software, textbooks, etc.) is expressly prohibited by law and subject to criminal penalties. In the event of detection of illegal actions, a report will be made to the Judicial Authority.

d. It is also forbidden:

- disseminate images, data or other material with pornographic, obscene, blasphemous, racist, defamatory and offensive content;
- use the ERSU data network and the services it offers for commercial purposes and for political or electoral propaganda;
- destroy or attempt to destroy, damage or attempt to damage, intercept or attempt to intercept or access or attempt to access without authorization the e-mail or data of other users or third parties, use, intercept or disseminate or attempt to intercept or disseminate passwords or access codes or cryptographic keys of other users or third parties, and in general committing or attempting to commit activities that violate the confidentiality of other users or third parties, as protected by applicable civil, criminal and administrative regulations;
- transfer large amounts of data, if not actually necessary;·
- do not set up access points to the network through the use of personal devices;

e. Do not manually configure the network settings of your device, the access infrastructure automatically assigns the necessary parameters to use the service. Manually configuring the parameters can lead to malfunctions of the connection for yourself and for other users.

f. Do not use the wireless network to carry out direct communications between users: the available bandwidth is not unlimited, keeping it busy for long-term communications limits the ability of other users to access the services more effectively.

g. The user must provide their device with adequate protection against viruses or other types of intrusions. The Entity assumes no responsibility for the data contained in the devices of the users of the service. In the event of an attack by a computer virus or other type of attack, the user will in no way be able to make a claim against the Entity. Users are therefore invited to install efficient and updated antivirus software and a suitably configured personal firewall on their equipment.