Sacred Heart College
MARIST OBSERVATORY
EDUCATION WITH HEART
Address: 15 Eckstein Street, Observatory, 2198, Johannesburg, South Africa
Email: info@sacredheart.co.za | Phone: +27 11 081 2200 | Website: www.sacredheart.co.za

# Computer and Internet Acceptable Usage Policy – Students

## Internet

Access to the Internet through the school network is a privilege. Users who are granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined below may be subjected to disciplinary action up to and including expulsion. Any inappropriate use that involves a criminal offense can result in legal action.

1. Internet is specifically limited to activities that support the educational and learning process.
2. If a student has any questions regarding the acceptable use, he/she should check with their teacher for additional guidance.
3. The internet shall not be used for any illegal or unlawful purposes, examples include downloading, distributing, transmitting any violent, threatening, defrauding, pornographic or obscene materials.
4. The internet shall not be used to infringe on any copyright laws with regards to downloading material.
5. The school email shall only be used for the conduct of school activities only. It may not be used to harass, intimidate or annoy another student or person even if it is related to school activities.
6. It must be noted that the school email is not guaranteed to be private. Messages transmitted through the school domain are the property of Sacred Heart College and therefore subject to inspection and control.
7. The internet shall not be used for performing work for profit or personal gain.
8. The internet may not be used to intercept or scan any network traffic.
9. The internet may not be used to circumvent or subvert security measures on the school network or any other network.

## Sacred Heart College Network (Intranet)

All students are given a username and password to log onto the Sacred Heart College network (intranet).

1. Students must only log in using their username and entering into their profile.
2. Students may log in at the MRC and the Computer Centres.
3. All students have access to their own “home” drive where they can store school related work only.
4. This “home” drive is limited only to school work as required for studying at Sacred Heart College in their subjects.
5. No personal files may be stored on the school network.
6. Any files that may be subject to copyright violations may not be stored on the school network. Examples would be songs, movies and digital textbooks not paid for.
7. If students identify or perceive an actual or suspected security problem, they must contact the Principal immediately.

8. Even if there is a perceived security problem/loophole, the student is required to do the right thing and not take advantage of the problem.



9. Portable storage devices (memory sticks / external hard drives) may only be used to transfer data from personal devices to the school network. This data may only be school related.
10. The student “home” drive is available to the teachers who need to view and assess the students work.

**Devices on Marist Brothers Network**

1. Devices placed on the network need to be named appropriately (Name Surname Device). Any devices with names that do not correspond with the student roll will be blocked.
2. Devices that use a VPN on the network will be removed.
3. Devices can be limited to their access to apps and internet as deemed necessary by Sacred Heart College
4. Sacred Heart College monitors all network activity of all devices joined to the network.

**Monitoring**

1. Students using the school's internal computer network must understand the following:
2. All users are entitled to reasonable privacy of their work under normal circumstances and therefore it is an offence to use or attempt to use another user's account/password no matter what the circumstances maybe.
3. Students are to conserve space by deleting unnecessary emails or other material which takes up excessive storage space.
4. Students should never download or install any software onto network drives. All copyright laws must be obeyed.
5. Students may not use any account other than their own. They have full responsibility for their accounts and must not share their passwords with anyone, and therefore, any violations of any part of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account.
6. Access to internet sites and internet content is filtered by the school’s firewall. The specific categories and rules of filtering are under frequent review by our Technical team. All internet activities are logged, monitored and archived by the IT Department. Extensive logs are kept of systems and activities on the network. The technical team may access all logs, and may review files and communications should the need arise, or if instructed to by the Principal.

The terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to the loss of network privileges and any other school disciplinary actions deemed appropriate.