SALESIAN COLLEGE ‘RUPERTSWOOD’

Computer Systems & Internet Access Authority

NAME __________________________________________

YEAR_______________ HOMEGROUP ___________

Please take the time to read the attached On-Line Access Policy, as it outlines the rights and obligations of all members of the Salesian College Community when they are accessing the Computer Systems and the Internet from within the College.

Return this (signed and dated) form to the College as soon as possible.

Parent/Guardian Signature: ______________________________

Date: ____________

By signing above, you are indicating to the College that you have read and agree to the conditions and obligations as outlined in the Salesian College “On-Line Access Policy”.

Student Signature: ______________________________

Date: ____________

By signing above, you are indicating to the College that you have read and agree to the conditions and obligations as outlined in the Salesian College “On-Line Access Policy”.

Note: Access to the colleges’ Computer Systems and Internet will not be granted to students until a correctly completed Computer Systems and Internet Access Authority has been returned to the College.

Office Use Only

Received Date: _____ / _____ / _____

Setup Date: _____ / _____ / _____
This page is intentionally blank
Salesian College On-line Access Policy

Information Technologies within Salesian College are highly valued facilities. The infrastructure to keep these facilities up and running costs many thousands of dollars each year to maintain and improve. Students and parents will have noticed the stability and improvements made to the system since the employment of a full time network manager. As the College moves into the next millennium, these improvements will continue at a rate that can be achieved within the current College budgetary regime. However, on very rare occasions, some students abuse and misuse them. As a result, we are publishing this policy on rules and responsibilities to coincide with the College’s connection to the Catholic Virtual Private Network (VPN). These rules and responsibilities will define and clarify issues to assist students and parents to more fully understand and be able to openly discuss this important area of College process.

Please refer to the ‘Student Code of Conduct “On-line Access Policy”’ and this document which details all banned on-line activities and their sanctions.

Students and parents should take particular note of the following points:

- Salesian College computer facilities and on-line access are to be used for educational research purposes only.
- Your username and password are for your personal use only and must not be shared with anyone. Any offences committed using your password will be regarded as your responsibility and penalties will be applied to the owner of the password.

All breaches of the College’s on-line access policy will result in sanctions. Listed below are some examples (refer to the ‘Student Code of Conduct’ for the full list). Students may also be suspended from school for an offence.

- **Hacking** – (essentially a criminal offence and potentially a police matter). All hacking matters will be discussed with the Principal or Deputy Principal - Students.
  - **Penalty** – Long term loss of use of network account (until the end of the current academic year). Information Technology students will have severely restricted and specified access to their accounts during Information Technology class time only.
- **Damage or Theft of Equipment**
  - **Penalty** – Determined by the Principal or the Deputy Principal - Students.
  - Payments for damages and long-term loss of use of network account (until the end of the current academic semester).
- **E-mail abuse**
  - **Penalty** – Will be linked to severity of the offence. Harassment of others is a breach of Student Code of Conduct and can be a criminal offence. Penalty may range from loss of network user account for two weeks to severely restricted access under written contract.
- **Using Another Persons’ Password or Account for Computer Access** – (essentially theft)
  - **Penalty** – 1st offence – Loss of network user account for four weeks.
  - Subsequent offences – severely restricted access under written contract.
- **Restricted File Access, Possession or Use** (eg. Offensive or copyrighted materials and pirated software)
  - **Penalty** – 1st offence – Loss of network user account for four weeks.
  - Subsequent offences – severely restricted access under written contract.
- **Computer Games, Possession or Use**
  - **Penalty** – 1st offence – Loss of network user account for four weeks.
  - Subsequent offences – Long term loss of network user account (until the end of the current academic semester).
- **Unauthorised Use of Computer Facilities for Commercial Purposes**
  - **Penalty** – these matters will be referred to the Principal or Deputy Principal - Students. Severe penalties may apply.

- **Use of Obscene, Harassing or Threatening Language**
  - **Penalty** – 1st offence – Warning.
  - **Subsequent offence** – Loss of network user account for 2 or more weeks.

**Process for Breaches of Rules**

1. All breaches of on-line access rules result in cancellation of the student’s on-line access throughout the College. A computer support staff member will usually do this without warning.
2. The student must initiate a discussion with the Year Level Co-ordinator before on-line access will be restored.
3. Computer support staff report offences to Year Level Co-ordinators / Deputy Principal - Students /Principal. Computer support staff are not required to discuss the matter or subsequent sanctions with students.
# Salesian College On-line Access Policy Definitions

<table>
<thead>
<tr>
<th>Offence</th>
<th>A list of the types of activities that describe the offence</th>
<th>Code of Conduct</th>
</tr>
</thead>
</table>
| Hacking (essentially a criminal offence and potentially a police matter)| The College’s network is divided into specific areas:  
- The area that students are authorised and encouraged to use and;  
- The area that is **out of bounds** as it is for operational or administration purposes.  
**Hacking is defined as:**  
- Any process that attempts to/successfully gains an individual or group, access to any part of the network that is out of bounds.  
- Any process that attempts to/successfully modifies or changes the operation of any part of the network.  
The network is defined as any server, hub, switch, cable, PC, tablet, notebook, router, access server, or any other equipment or device that the College or other companies have installed.  
The College logs key user activities and it is impossible to differentiate on our log files between an inquisitive person and a destructive individual. In business your employment would be **immediately** terminated if you attempted to gain unauthorised access or alter the operations of the business’s computer network.  
Examples of hacking include (but is not limited to):  
- Possession and/or use of any software like Telnet.  
- Software that traps passwords or gains unauthorised access to network equipment.  
- Software that searches the network for details of connected network equipment.  
- Actions which result in any denial of services on or to the network.  
- Activities or software that are detrimental to any equipment on the network.  
- Attempting to/opening directories or files on servers that are not for student use.  
- Attempting to/actually coercing Salesian student technicians to divulge network information.  
There is the opportunity to apply for student technician jobs.  
The best advice is, if you are unsure it probably means you should not be doing it and you need to get advise from IT management. NEVER accept and run software provided to you by other people if you do not know what it does!  
**Ignorance of the rules is no excuse.**  
| See the ‘On-line Access Policy’ section for further information on all the points listed on this page. |
| Damage or Theft of Equipment                                           | This is straightforward and self-explanatory. It relates to computer and network related equipment being deliberately damaged or stolen.                                                                                                                     | As above                                                                                                 |
| Using Another Persons' Password or Account for Computer Access         | It is unacceptable to loan your network logon password, make it easy for someone to get your password, to steal someone else's password or allow another person to use your computer account. As the owner of a network logon password **YOU** are responsible for its use and **YOU** must prove it was NOT you if your account is used to commit an offence. **One thing that has been observed all too often is that the person you trust the most is the one who is likely to get you in trouble.** Change your password often, especially if you suspect someone might know it! | As above                                                                                                 |
| Restricted File                                                        | - Any files, software or materials that breach the ‘Student Code of                                                                                                                          | As above                                                                                                 |
### Access, Possession or Use – including:

- Copyrighted
- Obscene
- Pornographic
- Offensive
- Dangerous
- Illegal
- Discriminatory – sexist, racist, etc.

#### Conduct’.

- *Music files of ANY band or solo artist are prohibited anywhere on the network unless YOU can prove beyond doubt that it is your own copyrighted work or is copyright free.*
- Any data that might be detrimental to yourself or others such as drug and bomb making.
- Possession of any copyright materials, songs, software, etc. that belongs to someone else and you have NOT paid for.
- Owning something at home does NOT mean you can legally copy OR use it at school.
- Storage, access or possession of any digital pictures or videos or text, etc., which could be offensive. BE WARNED – what you think as not offensive to YOU could easily offend someone else. If you are unsure, check with staff or better still, remove it permanently.

### Computer Games, Possession or Use

Computer GAMES are banned and NEVER to be RUN OR STORED on any PC, tablet or server in the College. This includes Internet type games that you might play on a Web browser.

### Unauthorised Use of Computer Facilities for Commercial Purposes

If you wish to put commercial materials on the network, get permission first and find out the correct process for doing this.

### Use of Obscene, Harassing or Threatening Language

This relates to obscene, harassing or threatening languages that might be electronically conveyed via e-mail, chat or any other voice, video, graphical or text format. A good example of this is the inappropriate use of software like NetMeeting.

### OOPS and BEFORE OOPS

1. Go to the Library resource centre and ASK if you are unsure about what is acceptable. We will be pleased to help and advise you.
2. If you accidentally do something that you think you should not have done, DEFINITELY come and tell us as this will probably mean no further action or sanctions will be applied.