ICT Acceptable Use Policy

Rosehill Secondary College's Computer User Protocol aims to support the ICT Mission by:

- Encouraging staff and students to employ good computer user practices and ethics.
- Maintaining a computer system that will provide the maximum amount of resources at any time.

GENERAL

1. Accessing, downloading and distribution of any material in violation of any college, state, federal or international regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening, harassing, or obscene material, pornographic material, or material protected by trade secret.
2. All communication and information accessible via the network should be assumed to be private property. Any sources used in research must be cited and credited to the author.
3. Users must respect others privacy and intellectual property (the same way you would respect another students workbook).
4. Students must have written parental/guardian permission to access the college network.
5. A Computer Network levy will be changed to all students who wish to access the network.

THE NETWORK

1. Network users will be issued with an account which can be used to access on – line information services. Each account owner is responsible for all the activity under that account including printing.
2. Network users will be issued with storage space on the server. All access to the network will depend on the username and password. Security for this area is the direct responsibility of the user and relies on the password remaining secret.
3. The Network Administrator(s) may review files and communication logs to maintain system integrity and ensure that users are using the system responsibly.
4. Users should not expect that all files stored on the school's servers will always be private and it is recommended that back – up copies be made on a USB storage device.
5. Actions not permitted on the College network are:

- Sending or displaying offensive messages (refer to the E/O Policy) or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or networks by physical abuse, introducing or creating viruses, altering source codes or software settings.
- Using other's passwords and trespassing in their work or files.
- Intentionally wasting resources.
- Using the network for unsanctioned commercial purposes.
- Using the network to disrupt its use by others.

THE USER

1. The user must accept responsibility for any time they are logged on to a computer. Therefore, you should log off if you are going to leave the computer for any period of time.
2. The user should exit any software application being used before opening another or logging off.
3. Each person will need to have a USB data storage device, as specified on the booklist, to store files. It is recommended that you save your work every 4 – 5 minutes to avoid loss due to electronic failure of either the computer or the network.
4. Each person is responsible for server disk space and should be downloading or deleting files that are no longer required in their folder (otherwise the Network Administrator(s) will be forced to clear space by deleting files.
5. The only people allowed to re-arrange any connections to the computers are the Network Administrator(s), the technician, teachers and the designated students. This includes such devices as cabling, keyboards, the mouse and the monitor.
6. Any problem with a computer or the network must be reported immediately.
7. Any problem with the security of the network must be reported to the Network Administrator(s) immediately and not demonstrated to others.

Failure to follow the User Protocol could seriously affect your ability to complete your work or your ability to access the system. It is in your interests to follow these guidelines and make sure that others are also being responsible. Any breach of this protocol will result in the possibility of the following sanctions.

SANCTIONS FOR RULE BREACHES

Depending on the severity of the damage/inconvenience, failure to follow the rules could result in:

- Withdrawal of privileges including on-line access
- Withdrawal from class
- Detentions
- Paying for or replacing damaged hardware
- Computer cleaning or maintenance

For serious breaches:

- Suspension
- Expulsion
- Law enforcement agencies involved