

## **Red Bend Catholic College Acceptable Use of Computers Policy**

### Introduction

At RBCC we recognize that Information Technology has become an integral part of our society and culture. We therefore provide a computer network to staff and students for the purpose of educational research and communication.

We need to ensure that staff and students of RBCC will become effective, efficient and appropriate users of the school network. It is expected that staff and students will become familiar with, and abide by, the Acceptable Use of Computers Policy. This policy is outlined in staff and student handbooks and on the College Website.

### General

The College computer resources are to be used for **Educational** and **College Business** purposes only.

You need a Username and Password to logon to the College computer network and it must not be shared with others. If you let others use your account they can change information you store on the network and introduce offensive or destructive material (viruses). Material placed on the network using your account will identify you as the person responsible.

You must avoid using technology in ways that:

- ▶ Intimidate, inconvenience, embarrass or offend other people
- ▶ Compromise the privacy, safety, health or well-being of others
- ▶ Reduce the overall quality of equipment or services available to the College Community
- ▶ Weaken or bypass security of any computer systems
- ▶ Undermine learning opportunities or fair assessment
- ▶ Breach copyright or other Australian law. This includes Plagiarism which is attempting to pass off someone else's work as your own.
- ▶ Intentionally waste resources
- ▶ Store unauthorized information on hard drives (c:\)

You may transfer educational material from another computer to the college computer network or vice versa. This could include Word, Excel or Publisher documents.

You must not transfer games or executable files (i.e. programs) to the college computers through floppy disks, email, storage devices or internet access.

You must not turn off any programs designed to protect the college network. This includes Antivirus and Monitoring software.

You must not install software on College Computers, only IT Staff can install software. IT Staff may wipe hard disk drives as part of computer maintenance in classrooms at any time.

Students and staff wishing to join their own computer to the College Network must organise this with IT Staff. A guideline is available with the recommended requirements from IT Staff.

Normal disciplinary procedures will apply to inappropriate use of the school computer network. This may mean suspending computer privileges for a specified time.

### Personal Storage

You are responsible for the contents of your personal storage space. To ensure you have maximum storage, regular maintenance and/or deletion of files is your responsibility.

Staff will view student files or activity when it is necessary for assessment or to investigate possible technical faults or suspected misuse of the resources.

Access to staff files is only permitted with written authority from the Principal and normally in the presence of the staff member involved.

All students and staff are responsible for backing up their own files and data. Computer failure and network problems will not be accepted as a reason for lateness with assignments.

### Internet and Email

Access to the internet is provided to all students. Levels of access will be determined, depending on curriculum needs.

Users that have access to email are required to create a folder in their workspace (Z:\My Documents). Users are encouraged to transfer email from the mail server to this folder on a regular basis.

When using e-mail as a means of communication, staff and students should apply the same professionalism, discretion and standards that they would expect in written business communication.

### Disclaimer

While every precaution is taken, RBCC makes no guarantees that the Network will be without faults. Data loss or interruptions to the system's accessibility may occur. Therefore users should always backup their work regularly.