Information Technologies Usage Policy

**Rationale:**
The aim and purpose of Information /Communication technology is to facilitate better learning. The school reflects the reality of the modern world in which we live-where the internet, electronic storage of information and the use of emails to communicate within a variety of forums and interested communities is now a part of normal life. The availability of such resources provides the opportunity for schools to help students develop their full potential: socially, spiritually, academically, emotionally and physically.

In accordance with the teachings of the Catholic Church, the practice of communication must reflect the highest standards of respect, truth, accountability and sensitivity for human rights.

Communication must always be courteous and truthful, since these values are integral to Christian belief and interaction with others. Truth is essential for individual liberty and for the building of authentic community among persons.

**Values:**
Truth, courtesy, accountability, justice, responsibility, respect, dignity and freedom.

**Policy Statement:**
The students and staff of MacKillop Catholic Primary School will be provided with access to email and internet facilities. Individuals will be accountable to each other and the Principal for the appropriate use of these technologies.

**Implementation Issues:**
1. MacKillop Catholic Primary School acknowledges that the availability of access to information provides a great opportunity for learning while at the same time posing a significant risk of inadvertent or deliberate exposure to inappropriate and offensive material. This risk is mitigated
by the school’s adoption of the Diocese of Rockhampton Intranet/Internet system of ‘Mysuite’, this is the system that the Year Levels (Prep- Year 7) have access to. This intra and interschool system have filter systems already installed, as well as, having a notification system that alerts the schools IT, on sight manager, of any attempts to access inappropriate sites. These monitoring and filtering systems ensure the children’s security and protected exposure to the outside world of the Net.

2. MacKillop Catholic Primary School is committed to ensuring that all students and staff are aware that unacceptable use of email and internet systems within the school environment will not be condoned under any circumstances and that disciplinary action will be taken against any person who breaches this policy.

3. MacKillop Catholic Primary School accepts that the use of email and internet systems must not infringe child protection policies, privacy legislation, anti-discrimination laws, anti-racism laws and copyright laws.

4. This policy works in conjunction with the MacKillop Catholic Primary School Bullying and Harassment policy.

5. Students and staff should be aware that all information kept on computers at MacKillop is the intellectual property of the school and the Diocese Catholic Education Office, and as such are subject to monitoring and accountability.

6. Students are required to hold an Internet Licence before accessing these technologies and be familiar with the Acceptable Use Guidelines. Prep- Year 3 learns about what Acceptable Use Guidelines are over their initial three years of Primary school. In Years 4-7 each child is required to read and sign a Computer Acceptable Use Guidelines- Students document at the beginning of each year.
7. MacKillop Catholic Primary School shall identify acceptable and unacceptable use of email and internet systems and is committed to regularly updating this policy.

8. Acceptable use may include:

- The facilitating, gathering and disseminating of information;
- encouraging collaborative projects and resource sharing;
- assisting technology transfer and fostering innovation;
- supporting education and research;
- fostering professional development;
- undertaking administrative functions;
- Any other tasks that support the school.

9. Unacceptable use would include but is not limited to:

- accessing networks without proper authorisation;
- transmitting or deliberately accessing and/or receiving material that may be considered inappropriate, including threatening, sexually explicit, or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally, including bullying or harassment of any other person (Cyber Bullying);
- communicating information concerning any password, identifying code or other confidential information;
- Interfering with or disrupting network users, services or equipment. Disruptions include but are not limited to, distribution of unsolicited advertising, propagation of viruses, in any form, and using the network to make unauthorised entry to any other machine accessible via the network;
- Breaching copyright laws, including software copyright and re-engineering of software.