STEWARDSHIP – STUDENT INFORMATION & COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE AGREEMENT

1.0 RATIONALE

In accordance with the teachings of the Catholic Church, the practice of electronic communication must be totally transparent and reflect the highest standard of accountability and sensitivity to human rights and relationships.

This ICT Acceptable Use Agreement serves to provide guidance to students of Mother Teresa Catholic College on the appropriate use, privacy, and access of electronic communications.

The scope of this ICT Acceptable Use Agreement applies to all College data, including stored data and other electronic means of communication. Such services include but are not limited to e-mail, SEQTA LMS, web portals, and social media operated by the College community.

2.0 DEFINITION

'Information and Communication Technology (ICT)' means the use of all computing hardware and software systems, digital services and data (including the internet and email) and telecommunication facilities that may be owned by the College or privately owned devices performing College business whilst a student of the College.

3.0 GUIDANCE NOTES:

- Students and Parents/Caregivers must accept the rules and regulations detailed in this document.
- Failure to comply with the rules could mean that access is withdrawn, or in some cases, more severe action is taken, including legal action, or loss of the student's place at the College
- Students must take responsibility for their own actions.
- Access to College owned or College supported ICT is only permitted for current students.
- Use of College owned or College supported ICT must comply with this acceptable use agreement.
- Students should not attempt to repair or maintain College owned computing equipment and peripherals including apple pencils, printers, mouse, keyboard etc.
- Students should not attempt to configure or manipulate any College owned digital services, systems and it's associated equipment and/or peripherals, including printers, mouse, keyboard etc.
- Students should back up their data to a suitable cloud resource such as iCloud or OneDrive to prevent data loss in case of device accidents/incidents.
- Students must report immediately to IT Staff any damage to equipment or peripherals.

4.0 ACCEPTABLE USE:

Subject to the following paragraphs, students may use the ICT facilities within the College for the purposes of data processing, communications, research and other applications of Information and Communication Technology that genuinely support the educational process in the College.

Monitoring and reporting

The College will oversee and administer the management of all student iPad devices. On all school days, restrictions will be imposed on the iPads, active from 8:30 am to 3:00 pm. This means that any non-sanctioned applications will be inaccessible during these designated hours, thereby ensuring an undisturbed academic environment. However, these restrictions will not be applied on a student's iPad on days when the student is not present at the College.

Students must be aware that all use of internet and online communication services can be audited and traced to the account of the user. All material on the iPad is subject to review by authorised

College staff. If at any stage there is a police request, the College will provide the authorities with access to the iPad and personal holdings associated with the use of the device.

Examples of unacceptable use, which could result in legal action and/or loss of place at the College:

- Use of the College's internet access, digital services or equipment for any illegal purpose.
- The acquisition, creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- The introduction of computer viruses, Trojans or worms, etc, with the intention of causing disruption or damage to:
  - College's equipment or data.
  - Third party equipment or data.
  - Privately owned user equipment that may be used regularly on site.
- Removal or attempted removal of College management or security protocols.

Any suspected security breach involving students, users from other schools, or from outside the Catholic Education network must also be reported to the College.

Examples of unacceptable use which could mean access is restricted or withdrawn:

- Use of impolite or abusive language in any form of digital medium.
- Allowing another student use of their College personal account and password.
- Accessing inappropriate chat sites and messaging sites including SMS messaging.
- Playing or downloading or sharing or use of the following:
  - Unauthorised/pirated Video games.
  - Unauthorised/pirated Music files including streaming audio.
  - Unauthorised/pirated Video files including streaming video.
  - Unauthorised/pirated Programs, Apps and executable files.
  - Unauthorised Programs/Apps/Websites/Digital Resources/Equipment on College premises.
  - Use of Virtual Private Networks (VPN).
  - Use Hotspot devices on College premises.

Cumulative breaches of policy will result in further disciplinary action. This list is by no means exhaustive and is given as a guide. The College will determine the category and severity of any instance of misuse.