1.0 Purpose

This document identifies the rights and responsibilities of those who use the electronic information resources at Saint Michael's College. This includes the networks, the on-campus information resources including telecommunications systems, and the Internet resources reached through Saint Michael's College systems.

2.0 Rights and Responsibilities

The Guest Network is not encrypted; therefore it is the responsibility of the user to ensure that no confidential information is downloaded or transmitted via email or social media. The user assumes all risk associated with the use of the un-encrypted network.

3.0 Unacceptable Use

The following activities are, in general, prohibited.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, network sniffing, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet, whether inside or outside the College's network.
- Using the Saint Michael's College system for illegal or criminal purposes.
- Unauthorized use of resources for commercial enterprises.
- Substantially and willfully interfering with another person's authorized use.
- Compromising or attempting to compromise privacy or confidentiality. In particular, attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness.

- Obstructing other people's work by consuming gratuitously large amounts of system resource (e.g., network bandwidth). This includes, but is not limited to, game playing or monopolizing information resources for entertainment or personal use.