IMMACULATE CONCEPTION SCHOOL – TECHNOLOGY ADMINISTRATION

ACCEPTABLE USE POLICY

1.0 Definitions.

1.1 **"AUP"** means this Acceptable Use Policy.

1.2 **"Facilities"** means the School's technology facilities, which include, but are not limited to, all computer and computer-related equipment, software, email facilities, facilities for internet access, on-line accounts, storage media, network accounts, computer and email files and messages, information processing and communications facilities, including those on School premises and those that are connected to or able to be connected to the School's facilities from locations off School premises, and any fax machines, telephones, smart phones, pagers, wireless email devices, copiers, scanners, or operating systems used in connection with the School's technology facilities.

1.3 **"Faculty"** means anyone currently employed by the School in any capacity, whether full or part time, whether paid or volunteer, who is not a Student at the School.

1.4 **"School"** means Immaculate Conception School, Annandale, New Jersey.

1.5 **"Spam"** means unauthorized and/or unsolicited electronic mass mailings.

1.6 **"Student"** means anyone currently enrolled as a student at the School at any time during the calendar year, regardless of whether school is in session.

2.0 Overview

The School has established the Facilities for the purpose of enabling Students and Faculty to pursue curriculum-related educational activities through the use of technology, such as accessing, processing, retrieving, and using information.

3.0 Purpose

The purpose of the AUP is to outline the acceptable use of the Facilities, at the School or from an offsite location, by Students and Faculty. These rules are in place to protect the Students, Faculty, and the School. Inappropriate use exposes the School to risks including virus attacks, compromise of network systems and services, and legal issues. Effective security is a cooperative effort involving the participation and support of every Student and Faculty member who deals with information and/or information systems in any way. It is the responsibility of every computer user to know these rules, and to conduct their activities accordingly.

4.0 Scope

The AUP applies to all current Faculty and Students (and, if applicable, a Student's parent or guardian who has received appropriate authorization from the School to use the Facilities), and continues to apply for as long as they remain Students or Faculty members, as the case may be. This policy covers all equipment within the Facilities, whether owned or leased by the School.

5.0 Policy

5.1 General Use and Ownership

1. Users should be aware that the data they create on the School's systems remains the property of the School. Because of the need to protect the School's network and systems, the School cannot guarantee the confidentiality of information stored on any of the Facilities.

2. For security and network maintenance purposes, authorized district personnel may monitor equipment, systems and network traffic at any time.

3. The School reserves the right to audit its networks and systems on a periodic basis to ensure compliance with the AUP.

4. The School reserves the right to access Student and Faculty files and communications within the Facilities.

5. Students and Faculty are permitted to use only the software to which they have been granted express rights by appropriate School personnel.

6. Students and Faculty must abide by any patent, copyright, or license restrictions that may relate to the use of the Facilities, products, programs or documentation.

7. Before leaving the School for any reason, Students and Faculty must return all software, accounts, and equipment provided to them by the School.

8. Any Student or Faculty member who becomes aware of any attempt to violate or bypass security mechanisms or effort to disrupt the network(s) must promptly report such activity to a teacher or class supervisor (if a Student), or to School security personnel (if a Faculty member).

5.2 Security and Proprietary Information

1. Each user must respect the privacy of information stored in the Facilities.

2. Each Student and Faculty member must use only the computer and software issued to himself or herself. If a computer is account is issued to a Student or Faculty member, that person must take responsibility to protect their account from unauthorized use.

3. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

4. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses or other computer attacks.

5.3. Unacceptable Use

The following activities are prohibited. The lists below are by no means exhaustive, but provide a framework for activities which fall into the category of unacceptable use. As an overall matter, it is strictly prohibited to engage in any activity that is illegal under local, state, federal or international law while utilizing any Facilities.

5.3.A System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 School.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, or the installation of any copyrighted software onto the local, floppy, or network drive for which the School or the end user does not have an active license, or otherwise using the Facilities to violate the terms of any software license agreement, or any applicable law.

3. Acquiring or modifying information that belongs to another person, or attempting to access restricted portions of the network(s) or operating system(s).

4. Introduction of malicious programs (such as viruses) into the network or server.

5. Revealing your account password to others or allowing use of your account by others. This includes family or other household members when working at home.

6. Making fraudulent offers of products or services from any School account.

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Student or Faculty Member is not an intended recipient or logging into a server or account that the Student or Faculty Member is not expressly authorized to access, unless these

duties are within the scope of regular duties. Circumventing user authentication or security of any host, network or account.

8. 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.

9. Providing information about, or lists of, Students or School employees to parties outside of the School.

10. Using the Facilities for commercial purposes, personal pursuits, discriminatory actions, illegal activities, solicitation, or accessing pornographic materials.

5.3.B Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding any "chain letters", "Ponzi" or other "pyramid" schemes.

6. Use of unsolicited email originating from within the School’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the School or connected via the School’s network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.0 Enforcement and Indemnification

6.1 Enforcement.

6.1.A **Faculty**. In addition to any punitive actions that may be prescribed by local, state or federal laws and regulations, and the indemnity in Section 6.2, any Faculty member who violates the AUP may be subject to disciplinary action, at the School's sole discretion, which may include (but is not limited to), temporary or permanent suspension from using the Facilities, termination of employment.

6.1.B **Students**. In addition to any punitive actions that may be prescribed by local, state or federal laws and regulations, and the indemnity in Section 6.2, any Student found to have violated the AUP may be subject to disciplinary action, at the School's sole discretion, which may include (but is not limited to) suspension from School; expulsion from School; removal from courses requiring use of Facilities; and/or receiving a failing grade in courses requiring use of Facilities.

6.1.C **Procedure**. In any instance of punitive action under this Section, the person accused of violating the AUP will be afforded due process in accordance with the School's standard administrative procedures.

6.2 Indemnification

Any Faculty member or Student (by way of parent or guardian) who has been found, after full administrative process, to have violated the AUP, shall indemnify and hold harmless the School, its directors, employees and agents from and against any losses, judgments, costs, attorneys' fees, penalties, claims, damages, suits and liability that relate to, or result from, the AUP violation.

7.0 Acknowledgement and Acceptance of the AUP

By signing below, I hereby acknowledge receipt of the AUP, and I agree to abide by all of its terms:

STUDENT NAME: (Print) _____

STUDENT SIGNATURE: _____

PARENT/GUARDIAN SIGNATURE: _____

FACULTY MEMBER NAME: _____