STATEMENT OF PHILOSOPHY

Miriam College is a trailblazing institution of learning that is committed to provide excellent academic programs imbued with the Maryknoll spirituality of Christian discipleship and mission, social responsibility, and values of Truth, Justice, Peace and Integrity of Creation.

Miriam College’s strategic direction towards fulfilling its significant role in leading innovation and transformation in Philippine education embodies the context of quality, relevance and sustainability. The quality of programs and implementation remains the top priority of the institution, which defines its high standard of education.

The primary goal of Miriam College in whatever circumstance is learning continuity and education for all. The school undertakes a consultative and collaborative decision-making process by coordinating with all stakeholders to assess the most appropriate and relevant decisions to undertake, especially during times of uncertainties.

The creation of the Virtual Campus at Miriam College is supportive of the institutional directions on innovation, inclusion, and relevance in today’s mission for the society, the learners and their respective families, the teachers, the staff, the school leaders, and the education partners that put meaning and purpose in the school’s existence.

POLICY

It is essential that MC is able to address the educational needs of the learners when they are affected by various circumstances. Learning Continuity (LC) is the educational management response of MC to ensure that the institution will not be vulnerable to disruptions. Its main priority is to protect the health and well-being of its students and employees while finding innovative ways to help students attain their educational goals. By presenting various pathways for LC, it is the goal of MC to continue to be committed in its vision to be a premier Filipino Catholic institution of learning that is responsive to the current challenges.

The current goal of MC is to provide a learning space and mode of delivery for students to continue their education, in the form of a virtual campus. It acknowledges that its students are currently located in various learning contexts; hence, the curriculum of the program offerings have been redesigned with versatility and flexibility as the main features of its content and mode of delivery.

The focus of LC is to engage students in a flexible learning which is a combination of online asynchronous and synchronous learning activities and when necessary, offline modalities that aim to achieve priority curricular goals per academic level. In this manner, students from preschool to graduate school will have access to continued education with greatest versatility for
independent or collaborative learning and interaction. Furthermore, in compliance with RA 10650, MC shall provide capacity building for all sectors of the community – from basic education to degree and technical-vocational programs -- in order to fully participate in LC.

MC believes that all the members of its community, especially the students, are a reflection of the school’s core values and principles. The students’ conduct and behavior, whether in the physical campus or virtual / online setting, must exhibit the ideals described by Mother Mary Joseph. For this reason, all existing school rules and regulations apply at all times, including in the online learning setting. This policy also adheres to other existing policies of the school regarding online behavior of students and employees covering the following areas:

- acceptable use and clear functions of gadgets
- proper care of gadgets
- safety features of the gadget

MC also implements the rules and regulations of Republic Act No. 10627, otherwise known as the Anti-Bullying Act of 2013, to prevent or manage cases related to cyberbullying as reflected in all Student Handbooks. Hence, anyone who sets a poor example and/or cause embarrassment or damage to school’s reputation or violate school rules in their online engagements will be subjected to an inquiry and disciplinary action if so warranted.

Miriam College will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate units/offices including but not limited to:

- Institutional
  - Data Privacy (Appendix A)
  - Data Management (Appendix B)
  - Employee Social Media Use (Appendix C)
  - MC Code of Conduct

- For BEU
  - HS Policy on the Use of the iPad (Appendix D)
  - MS Policy Guidebook on the Use of the iPad (Appendix E)

In cases of violations pertaining to the implementing guidelines, penalties or sanctions will be dealt with in accordance with the student handbooks of the different units, and the MC Code of Conduct and other existing policies (for employees) depending on the gravity of the offense.

**SCOPE**

This policy governs all members of the Miriam College community who are involved with LC.

Primary stakeholders of this policy are the students who are enrolled in the various units of Miriam College, and their parents. Students will be able to access materials and actively participate in activities prepared by their subject / course teachers.
Secondary stakeholders are the faculty, administrators, and administrative support staff. Aside from focusing on the delivery of academic content and student formation, secondary stakeholders must be able to provide online structures for research, consultation, counseling, career mentoring, peer and homeroom support. Optional interest-based materials and activities geared toward the development of leadership skills and the formation of Catholic-Christian values will be offered online as well.

GENERAL TERMS AND CONDITIONS

A. Framework
B. Definition of Terms

1. Institutional References

a. New Normal

This term is used to refer to the unfamiliar conditions brought about by a significant event or phenomenon, resulting to a new set of standards or expectations. A new normal is described in reference to how things have changed under new circumstances.

b. Virtual Campus

This refers to the portal webpage or website that provides students access to the learning materials and other resources.

c. Flexible Learning

Flexible Learning is a set of educational philosophies and systems, concerned with providing learners with increased choice, convenience, and personalization to suit the learner. In particular, flexible learning provides learners with choices about where, when, and how learning occurs. Sometimes also referred to as personalized learning, flexible learning includes both online and, if needed, offline modalities; the latter in consideration of students who may not have access to online learning.

d. Online Distance Learning

Online learning refers to education that takes place with the use of the internet, regardless of the physical location of the teacher and students. Related terms are e-Learning (learning with the help of electronic sources without physically visiting a classroom) and virtual learning (learning through the use of video conferencing software which can be attended by students at the same time or accessed at different times through its recording.)

Distance learning, also called remote learning, refers to learning that takes places off-campus or in a different location, when teachers and students are physically separated from each other, thus relying on the use of technology and internet-based tools and methods. In the case of our students, learning takes place at home.

Online distance learning, therefore, means that education is conducted through the use of the internet when teachers and students are not together in the classroom.

The following choices for the different aspects of the implementation of online distance learning:

- Modality: fully online with web-enabled F2F, transition to blended when conditions permit
- Pacing: self-paced, class-paced, class-paced with some self-paced
- Student-Instructor Ratio: <35 to 1
- Pedagogy: expository, practice, exploratory, collaborative
- Instructor Role Online: active instruction online, periodic presence online
- Student Role Online: independent self-paced study (listen or read, complete problems or answer questions, explore simulation and resources) or collaborate with instructor and/or peers
- Online Communication Synchrony: synchronous, asynchronous, or combination of both
- Source of Feedback: automated on LMS, teacher, peers
- Role of Online Assessment: determine student readiness for learning new content, instructional support, information on learning state, inputs to grades, and risk of failure

(Hodge, 2020)

e. Asynchronous Learning vs Synchronous Learning

Sometimes also referred to as location independent learning, asynchronous learning takes place when students learn the same material at different times and locations by providing access to the teaching materials, online platforms/tools for registration, instruction, communication and discussions, usually found in a common or shared learning space or portal.

Synchronous learning being the opposite of asynchronous is where students learn at the same time by giving them the opportunity to attend lectures through webinars, participate in video conferencing, live online discussions, etc.

Asynchronous online learning allows the learners to have a flexible time frame in accomplishing tasks, to adapt to self-guided lessons at their own pace, and to allow them to adjust and find delight in the new mode of learning while managing their other personal interests and concerns.

f. Blended Learning

A blended approach which combines online learning with in-person interaction is another learning modality that gives an option to have an opportunity for an in-person classroom interaction to ensure a maximum benefit through collaboration in a traditional learning process in bigger learning spaces while other learners alternately take on online learning. This approach may be adopted by MC should government and health regulatory groups deem face to face interaction safe.

g. Modular Delivery

This refers to courses or subject matter broken down into smaller units known as modules thereby reducing the cycle time of learning. These smaller units have their own knowledge and skills outcomes.

h. Hybrid Delivery

This refers to the practice of delivering courses online and then moving back to campus as the situation permits.
i. Digital Learning and Digital Assessments

Digital learning refers to the combination of online learning, e-learning, and blended learning along with the use of offline digital learning tools like cameras.

As a method or tool used in the teaching-learning process, digital assessments utilize tools, apps, and platforms to evaluate and measure student learning. This method/tool may be used to give ongoing feedback to students’ progress (formative assessment) and evaluate student learning at the end of a major concept or instructional unit (summative assessment).

j. Team teaching

This is an optional arrangement where two or more teachers collaborate in the preparation and delivery of lessons. Two or more teachers can be present in front of students, or take turns teaching a class. It is also possible that one teacher is assigned as the main instructor/facilitator of the class, and the other can serve as observer or resource person, or take over in case the first teacher is unable to continue. Arrangements may also be made for a tech mentor to assist faculty who are new to the technology being used during their online synchronous classes.

2. BEU Reference

Learning Partner

In a virtual class, the Learning Partner is an assigned adult outside the school community whom the student could rely on for assistance, guidance, and support in understanding and meeting the learning objectives and academic requirements. The Learning Partner may be a parent, guardian, or tutor.

C. Conditions of Learning Continuity

1. Institutional Conditions

   a. Teaching and Learning Environment

      1) Availability of Alternative Learning Spaces

      Students should be provided their own space in their home that is conducive for learning and participation in online activities. Likewise, teachers should also have ample workspace available for them. Such spaces should be comfortable, safe, and free from interruptions or hazards.

      2) Efficient Use of Modern Technology

      The programs are enhanced by modern technology which provides numerous options for students and parents to access the learning materials and participate in the learning activities, discussions, etc.

      Students and teachers should have a reliable internet connection and a designated desktop computer, laptop, or tablet assigned for their use. The
following are the recommended specifications, which shall be communicated to all students and teachers:

<table>
<thead>
<tr>
<th>LAPTOP/DESKTOP</th>
<th>MINIMUM / BASIC SPECIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Win7/Win 10</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel Core i3 or equivalent</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Screen Resolution</td>
<td>1024x768</td>
</tr>
<tr>
<td>Audio</td>
<td>Headphones with microphone</td>
</tr>
<tr>
<td>Storage</td>
<td>500 GB - up</td>
</tr>
<tr>
<td>Internet Bandwidth</td>
<td>1.5 Mbps - up</td>
</tr>
</tbody>
</table>

For a successful online experience (audio and video interaction), gadgets should have speakers, microphone, headset, and web camera. Its operating system should also allow for access to different types of learning management systems and applications.

b. Learning Management Systems and Applications

The educational units will each utilize their preferred and approved learning management system (LMS) and program applications that comply with the following criteria:

- Security and data privacy
- Functionality and adaptability
- Cost
- Accessibility / mobile friendliness
- Migration and integration
- Licensed source
- Reporting and analytics
- Customer support
- Simple / easy to follow user interface

c. Teacher and Student Support

The school shall hold learning sessions for faculty and students for orientation, exploration, and maximization of the chosen LMS and program applications.

The school shall also form an instructional support group composed of employees who have advanced technical skills to provide assistance to the faculty in the production of their instructional materials.

d. Flexibility in Implementing the Asynchronous or Blended (Asynchronous and Synchronous) Learning Approach

1) Shifting from traditional to online mode of learning

The school must observe a gradual implementation of an online arrangement. During the shift from the traditional face-to-face mode of teaching-learning to a
fully online arrangement, the school must first assess the conditions of all stakeholders and ensure everyone’s readiness prior to the full transition.

This scientific inquiry through survey, interview, observation, records, demographic information, trends, and other relevant sources is a collective approach which provides a pool of data to determine the appropriate learning intervention and modalities that the school adapts given the limiting condition of learning. The outcomes of the whole process of inquiry bring Miriam College to open up to the new frontier of out-of-the-physical classroom learning through online virtual platform vis-à-vis the offline-blended learning modality.

2) Implementation of Asynchronous or Blended (Asynchronous and Synchronous) Online Learning

The school shall adopt either the asynchronous or blended (asynchronous and synchronous) online learning approach in implementing LC.

Human connection, interaction, and routines play a vital role in holistic formation and in addressing the mental, emotional, psychological, and spiritual needs of students. Therefore, all teachers should provide an opportunity for regular online video conferences with students in smaller groups. This means that LC must still have some element of synchronicity, as required in the course.

3) Campus Wellness

MC shall continue to ensure that all members of the community are provided a safe and comfortable teaching-learning environment where activities are balanced for holistic development.

In the event of a long-term implementation of online learning, the school shall strengthen its structures to support the welfare, well-being, and needs of community members while maximizing technology and online platforms most especially in addressing mental and emotional health. Regular and periodic checks of both the social and IT infrastructure shall also be conducted. Any concerns expressed should be immediately addressed by unit administrators in coordination with the TWG on Learning Continuity.

e. Relevance of the Curriculum

1) Prioritization of content

The school curriculum will undergo review and recalibration to prioritize significant topics (knowledge and skills) in the learning plans without sacrificing learning objectives.

2) Learner-centered

Miriam College views the learner at the center of the educational process. The school understands that learners come from different contexts and their differences and disparities determine their varying capacities to adapt to
learning. Validation of outcomes from multiple scientific inquiries will ensure sound decisions and recommendations.

3) Multi-disciplinarity, inter-disciplinarity, and multi-dimensionality

Curriculum program developers must invest in finding connections across segmented or separate programs and activities, rather than offering them individually. The school must ensure the relevance of the teaching-learning experience.

4) Value-laden

The programs will remain to be infused with Christian values aimed at forming leaders in service who combine competence and compassion.

Academic concepts must be translated into real-life problems and solutions, and have strong integration with values formation. Doing so will not only create more meaning but also promote adaptability and yield greater sustainability in the long run.

5) Socio-emotional and essential skills

Whenever applicable, teachers should focus on building students’ essential skills (i.e., communication, leadership, problem-solving), emphasizing how one’s actions have effects on others. The earlier these concepts are understood by and ingrained in students, the more equipped they will be to adapt to this new normal.

f. Conduct and Etiquette

All members of the community shall continue to conduct themselves with appropriate and professional demeanor on all online platforms. This includes appearance and clothing, language and tone, non-verbal communication such as gestures and eye-contact, and the use of official / appropriate email addresses and handles.

g. Provisions for inequity and inaccessibility

The school shall exert maximum effort in reaching all learners to ensure that their education continues.

2. BEU Conditions

a. Home-school collaboration

Home-school collaboration is strongest in an online learning set-up. Because the home shall become the prime location of student learning, parents and teachers need to work together to help students with their needs and goals. All units shall have mechanisms in place to ensure efficient and effective home-school communication and collaboration.
b. **Consideration of accepted regulations**

The school shall take into consideration the limits on the amount of screen time set by the World Health Organization, which are as follows:

<table>
<thead>
<tr>
<th>AGE</th>
<th>SCREEN TIME</th>
<th>NOTES FOR PARENTS / LEARNING PARTNERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preschoolers</td>
<td>1 hour max per day</td>
<td>Resist the temptation to use screens to calm or distract. Consider print versions or other media versions. Ensure they understand what they are seeing and help them apply it to what is happening around them. Engage in creative play.</td>
</tr>
<tr>
<td>Elementary</td>
<td>1.5 hours max per day</td>
<td>Gradually allow students to plan and manage their time on and off the screen. Complement screen time with physical and creative activity and adequate rest.</td>
</tr>
<tr>
<td>Middle</td>
<td>2 hours max per day</td>
<td>Set screen time into a regular schedule.</td>
</tr>
</tbody>
</table>

*Source: American Academy of Pediatrics and World Health Organization*

c. **Creating new class schedules for online mode**

Once the transition to online learning has fully commenced, class and activity schedules, including deadlines of requirements, should allow for flexibility and varying rates of completion and submission. It must be assumed that online learning and completion of requirements will take at least thrice the length of time as compared to regular, face-to-face learning.

The school shall issue modified class schedules per unit which will reflect less required minutes per subject and less required subjects per day for the online platform. This will allow students to learn more at their own pace and give teachers more time to check on students, be available for consultations, and address concerns.

Provisions for non-academic co- and extra-curricular activities can be gradually introduced and implemented after the transition to online learning.

d. **Adjusting the grading system for learner-centeredness**

Alternative assessments appropriate to the online setting will be provided.

Bases for grading shall be adjusted by the respective unit academic committees, considering the students’ learning pace and capacity to complete requirements.
PROCEDURES

1. Creation of the Virtual Campus

The MC Virtual Campus (VC) is a learning portal where students can log in and access the following activities and resources:

- Recorded lectures and demonstrations created or curated by teachers
- Links to reading materials and learning supplements
- Academic consultations
- Spiritual formation
- Counseling services
- Online library
- Co- and extra-curricular activities including outreach and partnerships
- Peer support
- Career opportunities (for HEU students)

2. Guidelines for Virtual Campus Users

3. Specific Instructions related to the use of the Learning Management System (LMS)

4. On Site Work Resumption Protocols
Resources


Screen Time Guidelines by Age as recommended by the American Academy of Pediatrics (AAP) and World Health Organization (WHO). Retrieved April 27, 2020 from https://www.eyepromise.com/blog/screen-time-chart/


Contact Details for Questions or Concerns

For any questions or concerns, please contact any member of the Technical Working Group (TWG) for Learning Continuity:

- Dr. Jasmin Nario-Galace, Vice President for Academic Affairs
- Dr. Trixie Marie J. Sison, College of Education Dean
- Ms. Carol Ui, Administrative Director for Student Services and Academic Support
- Mr. Jose B. Maribbay, HEU Registrar
- Ms. Angela L. Cruz, Student Affairs Officer
- Ms. Elena Y. Flores, OVPAA Technical Assistant
- Engr. Dexter H. Llevarres, ICT Office Manager
- Mr. Romille Paul S. Alberto, Software Development Supervisor
- Mr. Jonathan A. Dineros, Technology and Infrastructure Supervisor
- Ms. Maria Jasmin B. Velasco, ICT Systems Management and Documentation Supervisor
- Mr. Marion Jude M. Gorospe, E-Learning Officer
- Ms. Maria Louella M. Tampinco, Director for Basic Education
- Ms. Glenda R. Villanueva, Miriam Adult Education Principal
- Mr. Alfred R. Sanchez, High School Assistant Principal for Academic Affairs
- Ms. Sofia Soledad G. De Guzman, High School Assistant Principal for Student Affairs
- Ms. Christine Joy Q. Corsiga, NUVALI Assistant Principal of Preschool to Grade 4
- Ms. Kristine Marie S. Lesaca-Saludez, Quality Assurance Office Faculty
APPENDIX A
National Privacy Commission (NPC) Privacy Toolkit (excerpts)

Internal weaknesses

Organizations can sometimes get too concerned with investing in the most updated and best information security software there is. What they fail to realize, however, is that any software becomes useless when vulnerabilities within the organization are not addressed.

Employee negligence

Without even resorting to sophisticated methods, perpetrators can use your unwitting employees as "portal" for their attacks. Considering organizations’ use of advanced security software, social engineering still proves to be a very cost-effective tactic for perpetrators. All they need do is identify and target the weakest link in the organization’s security chain, who are none other than your careless employees.

Some of the common mistakes employees make include having weak password, email, social media and web browsing practices. Cybercriminals exploit employees who do not use passwords, who use simple and short passwords, who use the same password across different services and accounts, and those who carelessly share passwords with others. Employees clicking on suspicious email links, social media content and website advertisements are also the easiest entry points to perpetuate malicious attacks discussed in the succeeding sections. Organizations also get exposed by employees’ poor security habits outside work such as the use of unsecured personal device to access work-related data, and the connection to unsecured wi-fi networks.

Employees also put their organizations at risk when they disregard well-crafted ICT standards and even the organization’s IT team. Critical errors under this category include doing unauthorized system changes, plugging unknown devices, downloading software and disabling security features—all without the IT team’s knowledge.

Weak or lack of information security policy

To avoid data breaches, it is desirable that an organization’s information security policies be always at par with emerging technology trends. Due to fast-paced changes, it is highly possible that no standards exist yet for handling these nascent practices. One such trend is the so-called “Bring Your Own Device” or BYOD.

Organizations allow BYOD in a desire to reduce costs and increase productivity, given the new-found IT self-sufficiency among employees. The setup allows employees to work and access corporate data using their own device, be it a laptop, ultrabook, tablet or smartphone. This frees up organizations from so much hardware, software, and device maintenance expenses. Presumably, it also empowers and motivates employees, given the ease, mobility, and flexibility of access that it makes possible. Organizations expect the resulting convenience and employee satisfaction to drive productivity levels up.

However, without adequate standards and employee preparations in place, BYOD puts corporate data at risk. This, especially in the absence of clear policies on who can access which data, and on what to do in case a personal device gets lost, stolen or compromised.

The lack of standards on the use of thumb drives or USB flash drives also poses a risk. It is a favorite storage device of perpetrators as it is small and concealable. Perpetrators can easily steal corporate data through these devices or use them to install malicious programs in computers.

Unrestricted access to certain corporate data also jeopardizes an organization’s security. For instance, access to sensitive employee information should be exclusive to the human resources department. This would make it harder for perpetrators to turn an employee into a portal of attack.

Malicious attacks
Phishing - This is a type of social engineering attack where cybercriminals pose as legitimate representatives of reputable organizations. The intent is to trick employees into divulging sensitive information that may result in data breach, identity theft and financial loss. Perpetrators carry this out through email, instant messages, phone calls, chat rooms, SMS, fake banner ads, message boards, fake job search sites and browser toolbars.

Malware - Malware is short for ‘malicious software’ which includes computer viruses, worms, Trojan horses, rootkit, ransomware, spyware, adware, scareware, among others. It is meant to infiltrate and infect computers to compromise device, disrupt service, steal data or monitor user activities.

Denial-of-service - A denial-of-service or DoS attack seeks to disrupt a network’s service and make it unavailable to its intended and legitimate users. This is done by flooding the network with useless traffic until it overwhelms the resources and crashes the system.

Man-in-the-middle - This is an attack designed to intercept communication between two parties, say a consumer and a website, in an attempt to impersonate both parties and steal valuable personal information.

Emerging attack platforms

Mobile - As a widely-used platform even in the workplace, mobile serves as a huge attack surface for perpetrators. The breadth of data found in mobile devices – contact information, photos, emails and other sensitive data, also makes them a primary attack target. The relative security weakness of mobile compared to personal computers increases its vulnerability.

Cloud - Similar to BYOD, cloud adoption in organizations has been on the rise. It is seen as a cost-efficient and effective measure to meet heightened computing needs. As cloud shifts organizations’ data and applications over high-capacity networks hosted in the internet, it helps reduce infrastructure and maintenance cost and improve manageability. However, it also serves as a new and easily accessible threat surface for perpetrators.

Internet of things - The internet of things or IoT is the concept of interconnectedness of physical devices ranging from cellphones, cars, ovens, washing machines, headphones, lamps, to wearable devices, via the internet. It espouses people-people, people-things and things-things relationships, intended to improve efficiency and promote a smart approach in doing things.

Combating data privacy threats

The National Privacy Commission has devised various means to address the above threats. These means are integrated into the “Five Pillars of Data Privacy Accountability and Compliance”, as discussed in the succeeding sections. This framework is not only meant to combat data privacy threats, but to also help personal information controllers and processors comply with the Data Privacy Act of 2012.

Encompassing organizational, physical and technical measures, the framework is aimed at helping develop an organizational culture protective of privacy.

Privacy Notice - It is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement, or privacy policy. As a privacy notice aims to empower the public and tell individuals what, how and why personal data is being collected from them, it should be highly readable to be effective. However, recent researches reveal that only a few actually read privacy notices.

Privacy notices should be concise and written in plain language as you write for a diverse audience. A segment of your audience may not be familiar with data privacy. Thus, it is important
to communicate the content clearly. If legal and/or technical terms are to be used, hyperlink these
to a definition. The notice should be concise, direct, and affirmative. Use short sentences in
active voice for easier understanding. If you are enumerating several items, use bullet points.
Each section of the notice should have an informative heading to accurately describe what
follows.

To reduce legal risks, privacy commitments in your notices should be aligned with your actual
privacy practices. Various resources reveal that while notices should try to avoid using bold
statements, they should not also be too generic. Notices should cover both current and
prospective privacy practices, which necessitates strategic planning involving everyone in the
organization.

The key is to conduct factual and legal due diligence.

What are the security requirements for a computer system?

1. Secure user authentication protocols including:
   a. Control of user IDs and other identifiers;
   b. Reasonably secure method of assigning and selecting passwords, or use of unique identifier
technologies, such as biometrics or token devices;
   c. Control of data security passwords to ensure that such passwords are kept in a location and/or
   format that does not compromise the security of the data they protect;
   d. Restricting access to active users and active user accounts only; and
   e. Blocking access to user identification after multiple unsuccessful attempts to gain access or the
   limitation placed on access for the particular system;

2. Secure access control measures that:
   a. Restrict access to records and files containing personal information to those who need such
   information to perform their job duties; and
   b. Assign unique identifications plus passwords, which are not vendor supplied default passwords,
to each person with computer access, that are reasonably designed to maintain the integrity of
the security of the access controls;

3. Encryption of all transmitted records and files containing personal information that will travel across
public networks, and encryption of all data containing personal information to be transmitted wirelessly;

4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;

5. Encryption of all personal information stored on laptops or other portable devices;

6. For files containing personal information on a system that is connected to the Internet, there must be
reasonably up-to-date firewall protection and operating system security patches, reasonably designed
to maintain the integrity of the personal information;

7. Reasonably up-to-date versions of system security agent software which must include malware
protection and reasonably up-to-date patches and virus definitions, or a version of such software that
can still be supported with up-to-date patches and virus definitions, and is set to receive the most
current security updates on a regular basis;

8. Education and training of employees on the proper use of the computer security system and the
importance of personal information security.
APPENDIX B
MC Policy QAO-001: Data Management (excerpts)

Creation

Institutional data generally falls into four classifications.

- School-Internal – Institutional data is generally classified as school-internal as default. Such data may be accessed and handled by eligible employees and designated appointees of the School in the conduct of school business. Access restrictions should be applied accordingly.

- Critical – These are data or types of information that require special handling and the highest level of protection such as all personally identifiable employee information and student education records, including grades. Improper or unauthorized access or handling of this data could result in criminal or civil penalties as stipulated in the data privacy law.

- Restricted – Selected or identified data that is accessible and handled only by authorized individuals or offices due to legal, ethical, or other restriction.

- Public - Data that may be accessed and used by the public has few restrictions and may be released upon request. Upon receipt of a request, the office seeks advice from the appropriate Data Steward. If the request is made pursuant to the MC open records statute, the recipient of the request seeks advice from the OVPAA, as well as the appropriate Data Steward.

Encoding and Accountability

Institutional Data will be kept accurate, complete, and current to the fullest extent that is practicable.

1. Security and Integrity of Institutional Data

   - Data Stewards and Data Users that possess or access Institutional Data accept full responsibility for the Institutional Data or subsets of Institutional Data that are in their possession and must adhere to the requirements to protect private sensitive and critical data from unauthorized access or loss.

   - Data Stewards and Data Users that access Institutional Data are responsible for the integrity, validity, and correctness of Institutional Data that are in their possession and must incorporate editing and validation checks to ensure the integrity and validity of such data. When Data Users identify errors in official Institutional Data, they must work with the Data Stewards and Custodians to correct the Institutional Data. If information that is derived from Institutional Data cannot be reconciled with the official Institutional Data, it cannot be considered official Institutional Data or presented as such.

2. File Naming Conventions

   - All members of the institution shall abide by the file naming conventions to ensure uniformity of storage and facilitate the unification of data
APPENDIX C
MC Policy RM-002: Employee Social Media Use (excerpts)

Implementing Guidelines

A. The use of social media by the individuals covered by this policy shall be guided by the following principles:

1. The exercise of one’s duty and responsibility to the different stakeholders of Miriam College should be the foremost consideration in creating and publishing contents, discussion, sharing of information and networking in any social media platform(s);
2. One’s social media activity should not violate any law related to copyright, data privacy, cybercrime and other regulations;
3. Respect for the right to privacy of the School’s stakeholders and demonstration of the highest professional conduct in social media activities are expected at all times;
4. Behavior in social media should be beyond moral reproach with utmost consideration given to students; and,
5. Employees should not act in a manner that will be unacceptable to Miriam College and its stakeholders as may be stipulated in the Code of Conduct for employees, and in current and future relevant issuances by Management, and in the provisions of the Data Privacy Act of 2012.

B. Social Media as Part of One’s Work

1. Employees using their social media as tools for their work must be well-informed of the subject matter of their social media posts, comments and other activities. Employees shall not initiate any activity which will spread or may spread misinformation, or violate any school policy.
2. Employees shall ensure that their opinions posted on social media will not disseminate misinformation or constitute a misrepresentation to their employment with Miriam College or to their profession.
3. Faculty creating social media accounts/groups for work-related purposes or activities must notify and seek the approval of their Direct Supervisors or they can already incorporate their social media accounts/groups in their official class syllabus or course outline. This is to protect the Faculty from any potential risks arising from their online interaction with students.

C. Professionalism in Social Media Use

1. The use the name, logo or other symbol of the School in social media shall at all times require approval from the Marketing and Communications Office.
2. Employees shall not accept/invite current students and their parents and product/service providers as contacts in their personal social media accounts. However, students who have graduated may be added to their accounts. Under special circumstances, where employees have existing social media connection with parents or product/service providers as relatives, friends, or classmates, may continue the connection with them and/or have them as future contacts in their accounts. For the sake of transparency, this should be discussed with their Direct Supervisors.
3. Online interaction with students should be limited to academic matters and shall be in the context of any official class conversation whether in social media account (e.g. Facebook group) or in email group (e.g. Yahoo group, Google Hangout or Viber group)
4. Personal data (i.e. personal information and sensitive personal information) concerning a student, colleague or any other stakeholder shall not be posted, shared or otherwise used in social media.
This includes anonymized information but with readily identifiable attributes that are recognizable by the concerned subject/s.

5. Faculty should not discuss grades, performance or personal information of students/colleagues on social media even if names have been removed.

6. Social media shall not be used to establish inappropriate relationships with students or other stakeholders.

7. Social media shall not be used to obtain information that would negatively impact on the reputation of the School.

8. Employees shall not post, share or use photos or videos taken which includes students, colleagues, or other stakeholders without explicit consent from individuals concerned. The consent requirement shall apply even if the other individuals concerned are not readily identifiable.

D. Responsible Social Media Activity

1. Employees shall not post or share obscene language and (material, or links to) sexually suggestive or sexually explicit material in their social media platforms;

2. Employees are prohibited from using their social media accounts to:
   • Defame, harass, stalk, bully a student, colleague or other stakeholders or commit other unacceptable behavior identified in the Code of Conduct for employees and students;
   • Post, share or use social media with the intent of damaging the reputation of a student, colleague or other stakeholders, especially if the subject is identified or identifiable. Likewise, derogatory comments will not be tolerated.
   • Post, share or otherwise use any information intended to be private or obtained through access to electronic data messages or documents;
   • Post, share or otherwise use recorded conversations between stakeholders, when such recording, whether audio or video, was obtained without consent of all the parties to the conversation.
   • Post or share contents (whether verified or unverified) that discredit a student, colleague or other stakeholders and likewise, violates the privacy of the subjects concerned.
APPENDIX D
HS Policy on the Use of the iPad

Acceptable Use

It is a must for each student to follow these guidelines and procedures insofar as the use of the iPad is concerned:

5. The iPad shall be used for the purpose of facilitating classroom learning experiences, completing subject requirements, and participating in selected school-related activities.

6. The iPad should not be used to access inappropriate sites and materials.

7. The intentional deletion or alteration of information or data of others, intentional misuse of system resources, and permitting misuse of system resources by others are strictly prohibited.

8. No software is to be loaded onto the tablet PC other than the one expressly approved by the Information and Communications Technology Office (ICTO) and the Academic Committee (Acad Com).

9. Software protected by copyright is not to be copied from, or by students using their personal iPad except as permitted by law or by the license or contract with the owner of the copyright. For this reason, rooting and jail breaking of applications are strictly prohibited.

10. Entertainment consoles, electronic games, and/or unlicensed softwares are not permitted to be installed in the iPad.

11. In light of personalizing the iPad, each student may choose her own wallpaper. However, this must be legally obtained, non-offensive, and mindful of the collective sensibility of the MCHS community.

12. Backgrounds may include pictures of friends, family, pets, vacation spots, etc. Pictures of violence, nudity, and disrespect for others are not acceptable.

13. Downloaded screen savers are known to contain spyware and viruses. Thus, they are not recommended.

14. The iPad is strictly for the use of the student to whom it is issued and should not be loaned to anyone else.
APPENDIX E
MS Policy Guidebook on the Use of the Apple iPad

It is a must for each student to follow these guidelines and procedures insofar as the use of the Apple iPad is concerned:

1. The device shall be used for the purpose of facilitating classroom learning experiences, completing subject requirements, and participating in selected school-related activities. It should be used to access only school-related sites and applications.

2. The intentional deletion or alteration of information or data of others, intentional misuse of system resources, and permitting misuse of system resources by others are strictly prohibited.

3. Each student may choose her own wallpaper however; this must be legally obtained, non-offensive, and mindful of the collective sensibility of the MCMS community. Backgrounds may include pictures of friends, family, pets, vacation spots, etc. Pictures of violence, nudity, and disrespect for others are not acceptable.

4. The device is strictly for the use of the student to whom it is issued and should not be loaned to anyone else.

5. The use of Apple iPad during recess and lunch is allowed for academic purposes only. However, students must use their device in designated areas only such as library and waiting area.