GORDON COLLEGE
Acceptable Use Policy for Information Technology (IT) Resources

As part of its educational mission, Gordon College acquires, develops, and maintains computing facilities, computer systems and application, web and mobile applications, and network platforms. These Information Technology (IT) resources are intended for college-related purposes, including direct and indirect support of the college's instruction, research, and services; administrative functions, student and campus life activities; and free exchange of ideas within the institution, local, national, and international communities.

I. POLICY STATEMENT

a. Computer systems and network are powerful technologies for accessing, processing and sharing information and knowledge. They are practical technologies for the current and future needs of Gordon College.

b. Computing facilities and network infrastructure are costly resources, that is why it must be used solely for college-related purposes such as instructions, research, and services; administrative functions, student and campus life activities; and free exchange of ideas within the institution, local, national, and international communities.

c. Information sharing is one of advantage since Information Technology allow individuals to access and copy information from remote sources, stakeholders must respect the rights of others particularly to their privacy and intellectual properties. Therefore, a need for rules and regulations to ensure equitable, secure, access to information, and maintained balance between privacy and freedom of information. The following regulations will govern the use of computing facilities, networks, computer systems and applications, and other Information Technology (IT) resources of Gordon College.

d. These regulation aims to:

- **i.** ensure an information infrastructure that promotes basic mission of Gordon College for college-related purposes, including direct and indirect support of the college's instruction, research, services; administrative functions, student and campus life activities; and free exchange of ideas within the institution, local, national, and international communities;
- **ii.** protect the integrity, reliability, availability, confidentiality, and efficiency of IT resources of Gordon College;
- **iii.** establish processes for addressing policy violations and providing sanctions for violators;
- **iv.** emphasize that Gordon College shall not be liable for any damages incurred form the use of its IT resources and for any claims and suits arising from the unauthorized and irresponsible use of the same;

v. warn stakeholders that use of IT resources for partisan political activities as defined in relevant rules and regulations of the Civil Service Commission or Gordon College, or for any unauthorized commercial purposes is prohibited; and

vi. notify stakeholders of the existence of this Policy.

II. DEFINITION OF TERMS

a. Agreement Form means document in which the user undertakes to comply with this Policy. The form may be electronic;

b. Confidential Information means data or information which on its face is not intended for unrestricted dissemination. Examples include student records, examination archives, proprietary technical information, disciplinary case records, administrative records, and the like;

c. Documents refer to forms, templates, records, lists, tables, reports, issuances, invoices, receipts, or other documents that contain personal information of data subjects;

d. Gordon College refers to the local college in Olongapo City through the mandate City Ordinance 07 Series of 2018;

e. Information Technology resources or IT resources includes computing facilities, hardware such as computer, terminals, printer, network structures, storage media, and software such as computer systems and applications, web and mobile applications, databases, files and information that are owned, managed, or maintained by any unit of Gordon College.

For the purpose of this Policy, any other equipment, hardware or software when attached to, or used to access and/or interact with any component of the IT resources of Gordon College may also be considered as part of its IT resources;

f. Private files mean information that a user would reasonably regard as private. Example includes the contents of electronic mail boxes, private file storage areas of individual users, and information store in other areas that are not public, even if no measure has been taken to protect such information;

g. Policy refers to the Gordon College Acceptable Use Policy for Information Technology (IT) Resources;

h. Stakeholder refers to a person with an interest or concern with Gordon College. It may be a student, parent/guardian, officials, employees, visitor, vendor, sponsor, donor, benefactor, etc;

i. **System and Network Administrator** means a person designated to manage a particular system assigned to the person, to oversee the day-to-day operation of the system, or to preliminary determined who is permitted to access IT resources;

j. **User** means part of stakeholders whether authorized or not, who makes any use of the IT resources or any of its components by any means or from any location.

III. SCOPE AND APPLICABILITY

a. General Coverage.

i. This Policy applies to Gordon College and all its Users.

ii. All Users should be aware of these regulations, and should realize that when using the IT resources within Gordon College, they are bound by these regulations. Users may be required to sign a form agreeing to comply with this Policy. However, failure to sign the agreement form will not release users from coverage of this Policy.

b. Local and External Conditions of Use.

i. Individual units within Gordon College may define additional or supplemental "conditions of use" for components under their control;

ii. These conditions must be consistent with this overall Policy but may provide additional details, guidelines, restrictions, and/or enforcement mechanisms. The individual units will be responsible for publishing the regulations they establish and their policies concerning the authorized and appropriate use of the IT resources for which they are responsible. Copies of these policies should be given to the College President, Vice-President for Administration and other concerned units and offices;

iii. Where use of external networks is involved, policies governing such use will be applicable and must be adhered to.

IV. GENERAL RESPONSIBILITIES

a. General Responsibilities of Users

In general, Users of Gordon College Information Technology (IT) Resources must;

i. use the IT system only for its intended purpose, and refrain from misusing or abusing it;

ii. maintain the integrity, reliability, availability, confidentiality, and efficiency of computer-based information resources;

iii. refrain from seeking gain unauthorized access or exceed authorized access;

iv. respect software copyright and licenses, and other intellectual property rights;

v. respect the rights of other Users; and

vi. be aware that although computing and information technology providers throughout the college are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate actions such as safeguarding their account and password, taking full advantage of file security mechanisms, back up critical data, and promptly reporting any misuse or violation of the Policy.

Stakeholders have an obligation to report suspected violations of the Acceptable Use Policy for Information Technology Resources should be directed to the MIS personnel or to the Vice-President on Administration and Finance.

b. General Responsibilities of MIS Personnel

You may refer to Gordon College Administration Manual for the complete details of MIS Personnel.

c. General Responsibilities of College Officials

i. To be informed and knowledgeable about these Policies

ii. To initiate systematic programs to inform academic and non-academic personnel of these policies.

V. APPROPRIATE USE

a. Appropriate Use

Users may only use the IT Resources of Gordon College for college-related purposes, including direct and indirect support of the college's instruction, research, services; administrative functions, student and campus life activities; and free exchange of ideas within the institution, local, national, and international communities. The particular purposes of any of the components of the IT Resource, as well as the nature and scope of authorized incidental personal use, may vary according to the duties and responsibilities of a User.

b. Proper Authorization

Users may access only those facilities and components of the IT Resources that are consistent with their authorization coming from competent authorities.

c. Specific Prohibitions on Use

The following categories of use of the IT Resources are considered prohibited and/or inappropriate:

i. **Uses Contrary to Law.**

1. **Unlawful use.** Users may not use the IT Resources for any activity that is contrary to any law or administrative rule or regulation, or to encourage any such unlawful activity. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal;

2. **Infringement of protected material.** Users must not infringe on the copyright and other property rights covering software, databases, and all other copyrighted material such as text, images, icons, retrieved from or through the IT resource. These acts shall include, but is not limited to, the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, unloading, downloading, uploading, communication, publication, or broadcasting of such material. Users must properly attribute any material they copy or through the IT Resources. Users are reminded that the infringement of intellectual property rights belonging to others through the use of telecommunications network is a criminal offense under Section 33(b) of the Electronic Commerce Act. Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal;

3. **Hacking.** Users may not use the IT Resources to gain unauthorized access into or interfere with another computer, system, server, information or communication system, or to obtain any access in order to corrupt, alter, steal or destroy any such system or information within such system or to introduce viruses. Users are reminded that all of the foregoing acts constitute the crime of Hacking under Section 33(a) of the Electronic Commerce Act and are punishable by mandatory imprisonment for one year to expulsion or dismissal. The penalty shall carry with permanent withdrawal of all IT privileges.

ii. **Uses Inconsistent with the Purpose of Gordon College**

1. **Cheating.** Users may not use the IT Resources to engage in cheating or academic dishonesty. Acts prohibited under this provision include but are not limited to the following:

    a. Copying a computer file that contains another person's work and submitting it for one's own credit;

b. Copying a computer file that contains another person's work and using it as a model for one's own work;

c. Collaborating on a work, sharing the computer files, and submitting the shared file, or a modification thereof, as one's individual work, when the work is supposed to be done individually; and

d. Communicating with another person online during the conduct of an examination. Violators shall suffer a penalty of suspension for not less that one semester. Student found guilty of cheating shall be barred from graduating with honors, even if their weighted average is within the requirement for graduation with honors.

2. **Political Use.** Users may not use the IT Resources for any partisan political activities. Violators shall suffer a penalty ranging from suspension for one month to one year.

3. **Unauthorized Commercial Use.**
   a. Users may not use the IT Resources for commercial purposes, except as permitted under other written policies of Gordon College or with the written approval of a competent authority;

   b. Violators shall suffer a penalty ranging from suspension for one month to one year with fine. If the violator is a student, the fine shall be P3000.00 or the amount equivalent to the earnings, whichever is higher. If the violator is a faculty member or an employee, the fine shall be one-half of his salary or the amount equivalent to the earnings, whichever is higher.

4. **Personal Use.** Users may not use the IT Resources for personal activities not related to appropriate college functions except in a purely incidental manner. Violators shall suffer a penalty ranging from suspension for one month to one year.

5. **Unauthorized gaming or entertainment.** Users may not play games or use entertainment software on or through the IT Resources unless authorized in writing by competent authorities. Violators shall suffer a penalty ranging from suspension for one week to one year; provided that the penalty for habitual offenses shall be expulsion or dismissal. The presence of game software or any part

thereof may be presumptive evidence of unauthorized gaming or entertainment.

6. **Use contrary to college policy or contract.** Users may not use the IT Resources in violation of other policies of the College, or in any manner inconsistent with the contractual obligations of the College. Violators shall suffer ranging from suspension for one week to one year in addition to the penalty of the offense facilitated through IT network.

iii. **Uses that Damage the Integrity, Reliability, Confidentiality, and Efficiency of IT Resources**

a. **Software and hardware installation and removal.** Unless properly authorized, users may not destroy, remove, modify, or install any computer equipment, peripheral, operating system, disk partition, software, database, configuration, or other component of the IT Resources; or connect any computer unit or external network to IT Resources. Violators shall suffer a penalty ranging from suspension for one month to expulsion.

b. **Unauthorized or destructive programs.** Unless properly authorized and part of User's administrative or academic duties, users may not develop or use programs on the IT Resources that may or intended to:

i. interfere with the ability of Gordon College to enforce these policies;

ii. damage any software or hardware component of the system;

iii. modify normally protected or restricted portions of the system or user accounts;

iv. access private or restricted portions of the system; or

v. interfere with or disrupt other computer users. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

c. **Destructive Acts.** Users may not attempt to crash, tie up, or deny any service on, the IT Resources. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

d. **Unauthorized Access.** Users may not attempt to gain unauthorized access, exceed authorized access, or enable

unauthorized access to IT resources, or to other networks or systems of which the IT resources is a part. Violators shall suffer a penalty ranging from suspension for one month to one year.

e. **Password protection.** A user who has been authorized to use password-protected account may not disclose such password or otherwise makes the account available to others without the permission of the System Administrator. Violators shall suffer a penalty ranging from suspension for one week to one year.

f. **Concealing access.** Users may not conceal, delete, or modify information or records pertaining to access to the IT Resources the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized used. Users may not conceal their identity or masquerade as other users when accessing, sending, receiving, processing, or storing through or on the IT Resources. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

g. **Prohibited material.** Users may not publish (on mailing lists, bulletin boards, and the World Wide Web) or disseminate prohibited materials over or store such information on the Gordon College IT Resources. Prohibited materials under this provision include but not limited to the following;

i. Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;

ii. Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer

iii. Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and

iv. Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

iv. **Uses That Encroach On the Rights of the Users**

a. **Wasteful and destructive practices.** Users may not encroach on others' access and use of the IT Resources

through wasteful and destructive practices such as but not limited to the following:

i. Sending chain-letters or excessive messages including spamming, either locally or off-campus; violators shall suffer a penalty ranging from suspension for one week to one month; spamming, includes the act of (1) repeated cross-posting the same message to as many newsgroups or mailing lists as possible, whether or not the message is germane to the stated topic of the newsgroups or mailing lists targeted, (2) maliciously sending out of unsolicited email in bulk, or (3) sending large unwanted or unnecessary files to a single email address.

ii. Printing excess copies of documents, files, data, or programs; violators shall suffer a penalty ranging from suspension for one week to one month;

iii. Running grossly inefficient programs when efficient alternatives are known by the user to be available; violators shall suffer a penalty ranging from suspension for one week to one month;

iv. Using more than one computer terminal at a time, unless specifically authorized by competent authority. Faculty members whose duties require the use of more than one computer shall be exempted. Violators shall suffer a penalty ranging from suspension for one week to one year;

v. Locking public access computers using screen savers or otherwise, unless specifically authorized by competent authority; violators shall suffer a penalty ranging from suspension for one week to one month;

vi. Not logging out of the system to allow other users to make use of the public access computer; violators shall suffer a penalty ranging from suspension for one week to one month; and

vii. Using a service which has been identified by the System Administrator as causing an excessive amount of traffic on the IT System or its external network links; violators shall suffer a penalty ranging from suspension for one week to one year.

b. **Offensive Material.**

i. Users may not use the facilities of the IT Resources to produce, disseminate, or display material that could

be considered offensive, pornographic, racially abusive, or libelous in nature.

ii. Users may not use electronic communication facilities (such as mail, chat, or systems with similar functions) to send messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of Gordon College. Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal.

c. **Inappropriate Messages.** Users may not send to a mailing list, including local or network news groups and bulletin boards, any unsolicited material inconsistent with the list's purpose. Users of an electronic mailing list are responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list are deemed to have solicited any material delivered by the list that is consistent with the list's purpose. Violators shall suffer a penalty ranging from suspension for one week to one month.

v. **Uses Which Violate Privacy**

a. **Confidential Information**

i. Unless properly authorized, users may not attempt to gain access to archives or systems that contain, process, or transmit confidential or sensitive personal information. Authorized users may not exceed their approved levels of access, nor should they disclose confidential information to others.

ii. Users shall treat as confidential such information which may become available to them through the use of the IT Resources, whether intentionally or accidentally. Users may not copy, modify, disseminate, or use such information, either in whole or in part, without the permission of the person or body entitled to give it. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.

b. **Encrypted Information.** Users shall consider as confidential all encrypted information. This includes but not limited to passwords, digital keys, and signatures. Users may not decrypt, attempt to decrypt, or enable others to decrypt such information if they are the intended recipient. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.

c. **Information Belonging to Others.** Users may not intentionally seek or provide information on, obtain copies of, or modify files, programs, or passwords belonging to other users, without the permission of those other users. Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal.

d. **Wiretapping, traffic capture and snooping.** Unless properly authorized, users may not re-route or capture data transmitted over the IT Resources. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.

vi. In addition to the penalties provided, all IT privileges of the offender may be suspended for the maximum period of the penalty. If the violation amounts to the penalty punishable by expulsion or dismissal, IT privileges may be revoked permanently.

vii. Repeated Violations of any of the acts proscribed under this policy shall be considered as "Gross Misconduct".

VI. TOLERATED USE

From time to time, the college may issue a list classifying certain types of use under the category of tolerated use. This list shall form part of this Policy and will be considered binding on all users. Users should consult their system and network administrators if they are not sure whether a certain type of us is considered allowed, tolerated, unacceptable, or prohibited.

VII. ENFORCEMENT PROCEDURES

a. Monitoring. Gordon College may monitor all use of the IT Resources at all times as may be necessary for its proper management. Activities on the IT Resources may be automatically and/or continuously logged. System and network administrators may examine these logs anytime. All logs shall be considered confidential.

b. Access to Private Files. Gordon College may access all aspects of the IT Resources, including private files, without the consent of the user in the following instances:

i. When necessary to identify or diagnose systems or security vulnerabilities, and problems, or otherwise preserved the integrity, reliability, availability, confidentiality and efficiency of the college;

ii. When such access to the IT Resources is required to carry out essential business functions of Gordon College;

iii. When necessary to avoid disrepute to Gordon College;

iv. When there are reasonable grounds to believe that a violation of law or significant breach of this Policy or any other policies of Gordon

College may have taken place, and that access and inspection may produce evidence related to the misconduct;

v. When required by law or administrative rules or court order; or

vi. When required to preserved public health and safety. The college will access private files without the consent of the user only with the approval of the College President except when an emergency entry is necessary to preserve the integrity, reliability, availability, confidentiality, and efficiency of the IT Resources or to preserve public health and safety. Gordon College through the system and network administrators will document all instances of access without consent.

c. Reporting Problems and Misuse. Users must report to the appropriate system administrators any defects discovered in the system accounting, or system security, all known or suspected abuse or misuse of the IT Resources, and especially any damage to or problems with their facilities or files.

d. User Cooperation. Users, when requested, are expected to cooperate with Gordon College in any investigation of IT system abuse.

e. Guidelines for Immediate Action.

1. **Notification.** When any system administrator or member of the faculty or employee has persuasive evidence of abuse or misuse of IT system, and if the evidence points to the activities or the files of an individual, he or she, shall within 24 hours of the discovery of the possible misuse, notify the College President or his/her duly designated authority.

2. **Suspension.** In such cases, the system administrator may temporarily suspend or restrict the user's access privileges for a period not exceeding 72 hours. A user may appeal such suspension or restriction and petition for immediate reinstatement of privileges through the College President or his/her duly designated authority. The College President may extend the suspension for thirty (30) days.

3. **Removal.** In addition, in such cases, the system administrator may immediately remove or uninstall from the IT Resources any material, software, or hardware which poses an immediate threat to the integrity, reliability, availability, confidentiality and efficiency of the IT Resources or any of its components or if the use might be contrary to this Policy. The user shall be notified of the action taken. A User may appeal such removal and petition for reinstatement of the material within fifteen (15) days from removal.

f. Investigation. The investigation and prosecution of academic and administrative personnel and students shall be in accordance with the regulation of Gordon College. The investigating committee, body or tribunal must have at least one member knowledgeable about Information Technology (IT). The actions the proper officer may undertake include but are not limited to the following;

1. Extend the suspension or restriction of a user's privileges for the duration of the investigation, or as may be deemed necessary to preserve evidence and protect the system and its users;

2. Call and interview potential witnesses; and

3. Summon the subject of the complaint to provide information.

g. Filing of Criminal Charges. In cases where there is evidence of serious misconduct or possible criminal activity, the College President shall file the appropriate criminal charges with the proper courts. Where proceedings have been instituted against a user for violation of this Policy, the College President may indefinitely suspend or restrict the user's access privileges for the duration of such proceedings.

h. Cumulative Remedies. The procedures under this Policy shall not exclude any other remedy available to any injured or interested party under any relevant law, administrative rule or regulation, or other policy of Gordon College.

i. External Legal Processes. Gordon College shall comply with any lawful order to provided electronic or other records or other information related to those records or relating to use of the IT Resources which may result from coercive processes in administrative investigations, or judicial actions or proceedings.

VIII. WAIVER

a. Loss of Data. Users recognize that systems and networks are imperfect and waive any claim for lost work or time that may arise from the use of the IT Resources. Gordon College shall not be liable for degradation or loss of personal data, software, or hardware as a result of their use of the IT Resources.

b. Authorization. Users recognize that Gordon College provides access to the IT Resources only as **A PRIVILEGE AND NOT A RIGHT**; that they have no right to use it for any purpose other than those directly connected with the mission of Gordon College; and that Gordon College may take whatever measures it deems necessary to enforce this. Users therefore waive any action they may have against Gordon College under any law or administrative rule or regulation for any act of the college undertakes this Policy, specifically including, but not limited to, those acts enumerated under Section 5.c. hereof.