HOLLAND COLLEGE
ADMINISTRATIVE REGULATION

Category:	**FISCAL, PHYSICAL AND INFORMATION RESOURCES**
Topic:	**Acceptable Use For Computing Resources At Holland College**
Code:	**20-07-1** *(Reassigned Jan2017 from 30-07-1)*
Effective Date:	**August 1 , 2017** **Revision: TWO**
Approved by:	**President of Holland College, Brian McMillan**

Related Documents:

Board Policy 20-07	(Information Technology Resources)
Administrative Regulation 20-07-2	(Holland College Website - Privacy Policy, PIPEDA and Terms of Use)
Administrative Regulation 40-01-1	Employee Code of Ethics and Conduct
Quality Procedure C09	Student Access to Computing and Networking Resources

Effective November 19, 2007, all new employees will sign-off in their Offer of Employment that they agree to be bound by all policies, regulations and procedures of the College. In addition to this general acknowledgement, the offer will expressly identify acceptance of two Administrative Regulations:

a) the Employee Code of Ethics and Conduct (AR-40-01-1), and
b) the Acceptable Use for Computing Resources at Holland College (AR-20-07-1).

Effective **July 2017**, the email sent to all students inviting them to activate their IT account with the College will include the following text:

> You must agree to abide by the terms & conditions of the Holland College Student Code of Conduct and the Acceptable Use for Computing Resources at Holland College. Click here to view a pdf of the documents.
>
> **A breach of any provision of the Code of Conduct or Acceptable Use Policy will be considered to be a disciplinary matter and subject to sanction in accordance with College Quality Procedures. By continuing with the activation of your Holland College student account you are hereby acknowledging that you have read, understand, and agree to abide by the Holland College Student Code of Conduct and the Acceptable Use for Computing Resources at Holland College.**

1. PURPOSE

1.1 The purpose of this regulation is to identify acceptable and unacceptable uses of the College's computing resources and to outline the process for dealing with allegations of illegal or unacceptable use.

2. DEFINITIONS

2.1 "Computing Resources" means all information technology owned, leased, operated, managed or licensed by the College, regardless of its location. It includes, but is not limited to, all IT infrastructure (such as network, printing, server, storage, backup, security, communications), all devices (such as personal desktop computers, laptop computers, tablets, mobile communications devices), all peripherals (such as printers, displays, audio visual devices), all software applications (such as administrative applications, desktop applications, cloud applications), all IT services (such as authentication, payment, information processing, technology support, subscriptions), as well as any data stored or transmitted on any of the above.

2.2 Integrated Technology Services: The use of the terms "Integrated Technology Services" and "ITS" in this document shall mean any member of the Integrated Technology Services department except where it specifically states the Manager of Integrated Technology r Services.

2.3 "Users" include current management employees, faculty, administration and support staff, currently registered students, and any others authorized as a User by the Manager of Integrated Technology Services, and who have entered into a User agreement.

3. BASIC PRINCIPLES

3.1 The College provides Computing Resources to Users for the purpose of furthering the College's academic mission, and conducting College business.

3.2 The College retains ownership of, or control over, all Computing Resources.

3.3 Limitations and/or restrictions imposed by the College on the use of Computing Resources are designed to ensure that they are used for legal purposes, that they are employed only for uses that are acceptable to the College, and to protect their availability, security, and integrity.

3.4 When using Computing Resources, each User of the Computing Resources must abide by all applicable laws, limitations and/or restrictions in this Regulation, and any other applicable College policies, regulations, codes of conduct, procedures and guidelines, and shall not aid or abet any other person's violation of this Regulation.

3.5 Violation of this Regulation may result in disciplinary action against a User, up to and including termination of employment, or dismissal from the College.

3.6 Limitations and/or restrictions imposed on the use of Computing Resources are subject to change by the College at any time.

3.7 The President is authorized to approve additional provisions with respect to the use of the Computing Resources which shall be documented as Procedures or Guidelines under this Regulation.

3.8 Any use of Computing Resources by a User is deemed to constitute acceptance of this Regulation.

4. AUTHORIZATION

4.1 All current management employees, faculty, administration and support, and current registered students, as well as approved guests, may access Computing Resources by obtaining proper College authorization.

4.2 A User shall employ only those Computing Resources (including individual computer and email accounts) for which the User has obtained proper College authorization, and shall use them only for the purposes intended.

4.3 Where password-protected accounts are used, each User will be held personally responsible for all activity for his or her account, regardless of who actually may be using the account at the time, unless the User can show that he or she used reasonable precautions to prevent others from gaining access to his or her account.

4.4 A User shall keep all passwords the User uses to access Computing Resources strictly confidential, shall not disclose them to any other person without the permission of Integrated Technology Services, and shall not store them on paper or electronically unless they are secured from unauthorized access.

4.5 Each User shall change their password(s) regularly.

4.6 A User shall not give, sell, or otherwise provide, any Computing Resource to any person who does not have proper authorization from the College for its use, or aid and abet any unauthorized use of Computing Resources by such a person.

4.7 Except in the case of authorized proxy access to email, a User shall not share computer or email accounts with any other person, without the written consent of Integrated Technology Services.

4.8 A User or other person shall not use unauthorized or false user names, passwords, computer addresses, or identities, or modify assigned network settings, to gain access to Computing Resources.

4.9 A User shall not connect any other equipment to Computing Resources without approval in writing from Integrated Technology Services.

4.10 A User may only access Computing Resources through means which have been formally made available by the College (wired, wireless or remote access using authorized accounts).

4.11 A User shall not setup personal methods of remote access to Computing Resources at Holland College (such as using remote access software) without express written permission from Integrated Technology Services.

4.12 Integrated Technology Services will conduct audits from time to time to detect the presence of software which allows remote access. Any unapproved software of this nature that is found on College equipment would be considered a serious breach of security.

5. PERSONAL USE

5.1 Computing Resources are provided to support the academic and business-related activities, of the College and its institutes and affiliates, and the activities of student organizations recognized by the College.

5.2 Occasional incidental personal use of Computing Resources is permitted as long as the User conforms to all applicable laws and this Regulation.

5.3 Computing Resources shall not be used by a User in connection with any personal business. The use of Computing Resources to sell goods, services, or information for personal gain, or to distribute advertising material for such a business, is strictly prohibited.

5.4 No User shall use the Computing Resources to advertise or solicit for any outside business, or organization that is not directly affiliated with the College.

5.5 No User shall use Computing Resources to enter into, or complete personal business transactions for profit (e.g. joining services that pay a User to surf the Internet).

6. ILLEGAL/UNACCEPTABLE USES

6.1 A User shall not use Computing Resources for any purpose or in any manner that would violate any law, including criminal laws, copyright laws, and intellectual property laws, any court order, or any licensing or other agreement to which the College is a party.

6.2 Computing Resources shall not to be used to deliberately access, create, transmit, store, copy, or distribute any information or material if doing so would violate a criminal law or would otherwise be illegal.

6.3 A User shall not deliberately use Computing Resources to view, copy, store or publish pornographic or sexually explicit material.

6.4 A User shall not use Computing Resources to deliberately display, transmit, distribute or make available or link to information that expresses or implies discrimination or any intention to discriminate, against any other person (including racist material or hate literature).

6.5 A User shall not deliberately use Computing Resources to access, view, copy, store, or publish information that promotes criminal, illegal, or violent activity.

6.6 Access to material mentioned in s. 6.4 or s. 6.5 by a student may be permitted if approved by the student's instructor as part of a student research project.

6.7 A User shall not use Computing Resources to send fraudulent, obscene, abusive, or harassing messages.

6.8 A User shall not make unauthorized copies of any software licensed to the College.

6.9 A User shall not download copyrighted material such as movies, music, etc. using Computing Resources, unless the material is required for College business and all terms of copyright have been met.

6.10 A User shall not deliberately or carelessly cause damage to Computing Resources.

6.11 A User shall not relocate any desktop computer without the permission of Integrated Technology Services.

6.12 A user shall not make changes to existing hardware/software configurations without approval from Integrated Technology Services.

6.13 A User shall not deliberately interfere with the work of other Users.

6.14 A User shall not deliberately overload, disrupt, or degrade the performance of Computing Resources (such as by distributing spam, chain letters, or pyramid solicitations), or waste Computing Resources (such as excessive streaming, downloading, or storage of data).

6.15 A User shall not use Computing Resources in order to gain unauthorized access to remote systems.

6.16 No User shall misrepresent his or her identity, or attempt to impersonate others, when using Computing Resources.

7. PRIVACY

7.1 Privacy is an important College value, however, privacy in the use of Computing Resources can not be guaranteed.

7.2 A User may normally expect that the User's communications will be treated as private, and that they will not be accessed without his or her permission.

7.3 The College does, however, reserve the right, consistent with this Regulation, to access, review and disclose electronic information that is transmitted over, or stored on Computing Resources in certain limited situations.

7.4 The Vice President of Corporate Services may request in writing that Integrated Technology Services provide access to a Computing Resources (including computer, email, and voicemail accounts) or any equipment connected to Computing Resources, without the consent of the employee or student concerned when access:

a) is necessary to comply with any legal requirement or process (such as a court order); or

b) is required to carry out an investigation or disciplinary proceeding pursuant to s. 11 of this Regulation; or

c) may provide information required to deal with an emergency; or

d) in the case of an employee, will yield information that is needed for the ordinary business of the College to proceed. (For example, where an employee is absent or has left the College, and the information required is not available elsewhere).

7.5 Privacy also does not extend to situations which Integrated Technology Services requires access to Computing Resources or any equipment connected to Computing Resources:

a) to gather sufficient information to diagnose or correct network, hardware, or software problems, or to perform other maintenance tasks;

b) to monitor levels of network traffic, use software that logs network activity, to routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, and network loading, to make copies of files and maintain archives of those copies, and to perform other tasks as a normal part of system administration;

c) to perform tasks required to maintain the integrity of Computing Resources.

7.6 If the performance of any task under s.7.5 requires that Integrated Technology Services log on to a User's account, the User's password will be changed and the User will be notified of the change.

7.7 Like the members of the College community, employees who support and provide Computing Resources are expected in the normal course of business to use Computing Resources appropriately, respect the privacy of others, and maintain the privacy of information that may come to their attention during the routine exercise of their duties.

7.8 Each User shall respect the privacy rights of other Users.

7.9 No User shall deliberately seek information on, obtain copies of, or modify files or data belonging to other Users, without permission from that User.

8. SECURITY

8.1 Each User shall comply with all security requirements that apply to Computing Resources.

8.2 No User shall attempt to subvert or circumvent College security measures (passwords, firewall, hardware locks, etc.)

8.3 Each User shall ensure that he/she is logged off his or her computer anytime he or she is away from his or her desk (even for short periods of time).

8.4 Except when accessing Wi-Fi networks with an approved account, no electronic device shall be connected to the College's network (personal computer, wireless router, IP addressable device, etc.) without the express written permission of Integrated Technology Services.

8.5 Each User is responsible for maintaining the security of any College data which may reside on a computing or storage device they may be using (such as a desktop, laptop, tablet, USB key, cloud storage, etc.), and shall take reasonable measures to prevent access by unauthorized persons. Both physical and electronic access must be restricted to authorized persons only.

8.6 Users must ensure that all corporate data resides on an approved networked storage device (not locally) and is available to be backed up by Integrated Technology Services on a regular basis. Users of mobile computing devices must ensure that all corporate data is uploaded to an approved networked storage device on a frequent basis so as to minimize the potential of data loss.

8.7 Users should not, except when necessary for College operations, store information considered to be private or confidential on mobile or cloud computing devices.

8.8 A User of mobile computing devices is responsible to ensure they have up-to-date anti-virus programs running on their systems so as to minimize the possibility of infecting College networks from the inside.

8.9 Any port scanning, network mapping, penetration testing, or other indiscriminate analysis, of the College network is strictly prohibited.

8.10 A User shall not load daemons/services on any computer to act as a server (Mail servers, Web Servers, Peer to Peer servers including music/video sharing servers and IP telephony peers such as Skype, DNS, DHCP, Remote access, etc.), without express written permission of the Manager of Integrated Technology Services.

8.11 A User shall not load personal firewall software on their PC as it disrupts communication with some of the network utilities presently used by Integrated Technology Services.

8.12 Should a device or media containing College data be lost or stolen, the User's immediate supervisor and Integrated Technology Services must both be notified as soon as possible.

8.13 Any User who becomes aware of a breach or potential breach of computer/network security, (attempted hacking, compromised accounts, etc.), must notify Integrated Technology Services immediately. Failure to do so may result in the User being found to have participated in any breach.

9. TERMINATION OF ACCESS RIGHTS

9.1 Integrated Technology Services will terminate a User's access to Computing Resources if requested by a User's supervisor, due to the suspension or termination of the User's employment, student, internship, or volunteer, status with the College.

9.2 A User should make arrangements with Integrated Technology Services to remove or to retain all personal data and files prior to leaving the College.

9.3 Once a former User has left the College, the College disclaims any and all responsibility for such personal data and files.

9.4 Failure to remove such data or files may also result in their removal by Integrated Technology Services.

10. DISCLAIMER OF LIABILITY

10.1 The College makes no warranties of any kind, either express or implied, that the functions or the services provided by, or through, the Computing Resources will be error free or without defect. The College will not be responsible for any damage Users may suffer, including, but not limited to, loss of data or interruption of services.

10.2 The College is not responsible for the accuracy or the quality of information obtained through or stored on its computer network.

10.3 The College is not responsible for any financial obligations incurred or arising through a User's use of its Computing Resources.

10.4 The College is not responsible for the content of the communications of any person utilizing Computing Resources.

10.5 A User shall be held liable for any costs, claims, and liability the College, its officers, agents, or employees, incurs as a result of the use of Computing Resources by the User.

11. ENFORCEMENT

11.1 The Manager of Integrated Technology Services or designate may become aware of a suspected violation of this Regulation, through a report, complaint, or in the normal course of operations. Integrated Technology Services Staff (ITS) are designated by the Manager of Integrated Technology Services to deal with immediate threats and report to the Manager as soon as possible.

11.2 In the event of a suspected violation, ITS STAFF shall initiate a preliminary investigation to determine if sufficient grounds exist for further action.

11.3 The Manager of Integrated Technology Services will notify the instructor or supervisor of a User suspected of a violation of this Regulation that the User is under investigation. The instructor or supervisor will notify the User unless, in opinion of the Manager of Integrated Technology Services, providing notice would compromise the investigation, or would present a significant risk of harm to Computing Resources or a person.

11.4 If, in the opinion of the ITS STAFF, the security or integrity of any Computing Resources is at risk, or if there is a suspected violation of the law or any agreement, the ITS STAFF may take such reasonable measures as he or she deems appropriate pending completion of the investigation (including locking an account or access point, or removing material that is suspected to be in violation of the law or an agreement). The ITS STAFF will document the incident and any action taken and, as soon as possible, inform the Manager of Integrated Technology Services of the situation.

11.5 If the preliminary investigation requires the examination of programs, files, data, tapes, or passwords of a particular User, the Manager of Integrated Technology Services will review the situation with and get the approval of one of the following College officials as applicable, before proceeding with the examination:

User		Official
Student	-	Vice President of Corporate Services
Employee	-	Vice President of Corporate Services
Others	-	Vice President of Corporate Services

11.6 Upon completion of the preliminary investigation, the applicable College official will give the User suspected of the violation an opportunity to provide an explanation and, thereafter, the College official may take one or more of the following steps:

a) if there is no evidence of a violation of this Regulation found, no action will be taken other than to inform the User and the complainant, if any, of the decision;

b) if there has been a violation of this Regulation, but the offence is not serious, or was accidental, the College official shall inform the User of that decision, and will direct the User to discontinue the activities that have been found to be in violation;

c) if the College official determines that the User has violated this Regulation and that the offence is serious (such as where it involves a violation of the law), if there is a pattern of repeated misuse, or if the User has or is refusing to comply with the direction of College, the matter will be referred to the applicable College official (see par. 11.5) who will initiate the appropriate disciplinary process;

d) the appropriate disciplinary process, in the case of an employee, is the normal process used for cases involving employee misconduct, and as prescribed in the applicable collective agreement;

e) the appropriate discipline process, in the case of a student, shall be those normally used in cases involving student misconduct and set out in the Student Code of Conduct.

11.7 The sanctions available for any breach of this Regulation include those normally available in employee and student misconduct cases, and can include termination of employment, or dismissal from the College. Additional sanctions that may be imposed include:

a) temporary or permanent removal of, or limitations on the right to use Computing Resources, or particular Computing Resources;

b) removal of material that violates this Regulation from Computing Resources;

c) a requirement that the cost of replacing damaged Computing Resources, including labour and materials, be paid.

11.8 In addition, if the suspected breach of this Regulation involved a suspected breach of the law, the College may report the matter to the appropriate law enforcement agencies.

11.9 Any investigation or disciplinary proceeding pursuant to this section may involve collection and analysis of information that would otherwise be considered private.

12. REQUEST TO DEVIATE FROM THIS REGULATION

12.1 If, in the opinion of the Vice President of Corporate Services, compliance with a particular provision of this Regulation would limit legitimate educational or business usages of Computing Resources, the Vice President of Corporate Services after seeking the advice of the Manager of Integrated Technology Services, may give written permission to deviate from this Regulation.