IT ELECTRONIC MAIL POLICY

IT ELECTRONIC MAIL POLICY			
Effective Date	May 19, 2016	**Cross-Reference**	1. Communication Policy 2. Records Management Policy 3. Protection of Privacy Policy 4. Record Classification and Handling Policy 5. GPRC Style Guide
Responsibility	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. Email Etiquette 2. Email Acceptable Use

1. Policy Statement

1.1 Grande Prairie Regional College ("GPRC" or the "Institution") is committed to supporting and providing email systems for communication. Electronic communications must follow the same professional standards as any other formal business communication to ensure productivity, meet user and partner expectations, prevent breach of confidentiality or privacy, and comply with contractual and legal requirements.

2. Background

2.1 Email is one of GPRC's core internal and external communication methods. However, misuse of email can present risks, such as:

2.1.1. A confidential (or privacy) breach, by sending a sensitive attachment in an unprotected format, or sending the file to the wrong person.

2.1.2. Potential of litigation when sending an inappropriate email.

2.1.3. Presenting a poor image of the Institution or its employees by not following professional communication standards and styles (e.g. sending a message that is poorly written or containing typos).

2.1.4. Impact on business operation productivity resulting from inefficient communication, such as not clearly articulating ideas, requests, facts or information.

3. Policy Objective

3.1 It is important for users to understand the appropriate use of electronic communications. The purpose of this policy is to define a minimum set of rules to be followed by all GPRC staff when using email.

4. Scope

4.1 This policy applies to:

4.1.1. All Institution offices, campuses and learning centres.

4.1.2. All students, employees, consultants, contractors, agents and authorized users accessing Institution IT systems and applications.

4.1.3. All email transmitted, processed or stored through:

4.1.3.1. Any Institution computer, smartphone or IT system

4.1.3.2. Any other technology, managed by the Institution or not, containing Institution information

5. Definitions

5.1 Electronic mail ("Email") refers to the electronic transfer of information between various users. Email can be used to transfer text or any other electronic media, such as pictures, video, recording, etc.

5.2 "Users" are students, employees, consultants, contractors, agents and authorized users accessing GPRC IT systems and applications.

6. Guiding Principles

6.1 Users must not use email for illegal, disruptive, social or political positioning, unethical or unprofessional activities, for personal gain, or for any purpose that would jeopardize the business interests of GPRC.

6.2 When writing emails, users should follow the Communications Policy and the guidance defined in Appendix 1 – Email Etiquette.

6.3 When writing emails, users must comply with Appendix 2 - Email Acceptable Use.

6.4 Emails that are used for the purposes of a "formal record" must follow the requirements of the Records Management Policy as well as specific *legislation which may affect retention requirements, such as the Limitations Act*, *Evidence Act*, and *Income Tax Act*.

6.5 Email messages sent out using GPRC IT systems are never to be considered as personal and private. Email system administrators may access an employee's email for various reasons, including:

6.5.1. For a legitimate business purpose, such as the need to access information when an employee is absent for an extended period of time.
6.5.2. For a legal inquiry. Professional emails may be released to the public in the event of legal inquiries. All emails, including personal communications, may be subject to discovery proceedings in legal actions or provided in response to an access request under the Alberta Freedom of Information and Protection of Privacy Act.
6.5.3. To diagnose and resolve technical problems involving system hardware, software, or communications.
6.5.4. To investigate possible misuse of email when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

6.6 Users will manage all e-mail communications in accordance with the Records Management Policy.

6.7 Emails that are intended to promote or market GPRC to potential customers where revenue could be generated are subject to the Canadian Anti-Spam Legislation, and must be in full compliance at all times. Additionally, mass marketing email are subject to the internal guidelines set out in the Web Style Guide. To ensure compliance with both standards, new and existing initiatives must be formally approved by the Corporate Communications Officer.

7. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy.
Vice-President, Administration	• Review and formally support this policy.
IT Director	• Develop and maintain this policy. • Take proactive steps to reinforce compliance with this policy by all stakeholders. • Review and approve any exceptions request relative to the requirements in this policy.
Institution Management, Supervisors or Representatives	• Explain the terms of this policy to employees and students and assist users to understand the requirements of this policy. • Ensure that all users follow the requirements of this policy.
Contract Administrators and Managers	• Follow the guidelines provided in this policy when performing due diligence and assessment of the risks related to security for any new contract. • Ensure that responsibilities and obligations of each party to the contractual relationship are outlined in the contract executed between the Institution and the contractor/sub-contractor.
Human Resources	• Present each new employee or contractor with the existing GPRC policies upon the first day of commencing work. • Support all employees and students in understanding the requirements of this policy.
All users (Employees and contractors, Students, Visitors and or Volunteers)	• Comply with the applicable requirements of this policy at all times. • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible.

8. Exceptions to the Policy

8.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

8.2 Policy exceptions must describe:

8.2.1. The nature of the exception

8.2.2. A reasonable explanation for why the policy exception is required

8.2.3. Any risks created by the policy exception

8.2.4. Evidence of approval by the IT Director

9. Inquiries

9.1 Inquiries regarding this policy can be directed to the IT Director.

10. Amendments (Revision History)

10.1 Amendments to this policy will be published from time to time and circulated to the College community.

Appendix 1 – Email Etiquette

1. When writing an email:
   1.1. It must contain a meaningful subject line that helps clarify what the email is about and helps the recipient prioritize reading your email.
   1.2. Write clear, short paragraphs and be direct and to the point.
   1.3. Be friendly and cordial.
   1.4. Do not make inappropriate jokes or witty remarks.
   1.5. Take care to use emoticons without excess.
   1.6. Use spell-check to remove typos, correct punctuation and grammar.
   1.7. Take care when using capitalization or exclamation points.
   1.8. Include a signature with your name, role and contact information.
   1.9. Double-check the intended recipient(s) before sending.

2. When responding to email:
   2.1. Respond within a reasonable time frame, generally within one business day. If you cannot answer a specific request, leave a reply indicating that you have received the email and will be answering at a future time (end of day, end of week, etc.).
   2.2. Do not hit "reply all" unless every member on the email chain needs to read your email.
   2.3. Keep a neutral and professional tone and avoid any “flaming” or excessive outpouring of information in reaction to personal feelings or emotions.
   2.4. Keep a copy of the previous email but delete the trail of older messages where possible, to keep your response clean.
   2.5. It may be easier and more practical to embed answers into the sender's message at the bottom of the email. When doing this, ensure you:
      2.5.1. Clearly state so at the top of your email.
      2.5.2. Change the color of the text to distinguish the answer from the question.
      2.5.3. Use spacing between the answer and the question.

3. Sensitive data in email:
   3.1. By default, email is not encrypted and can be potentially read by an unintended person. As a result, sensitive information must never be sent unprotected by email.
   3.2. Users must follow the Record Classification and Handling Policy.
   3.3. Users must contact the Help Desk for any question on how to protect sensitive information to be sent out by email.

4. Email attachments.
   4.1. Inform the recipient of your intention to send a large attachment before doing so.
   4.2. Use a file transfer system that is approved by the Institution.
   4.3. Avoid unnecessarily large attachments and use a compression tool to limit the size of such attachments. Consider:
      - “Zipping” or compressing files and documents before sending.
      - Saving electronic pictures and graphic media in a compressed format (“png” or “jpeg” instead of “raw” or “bmp” for pictures) or resize such media.
   4.4. Name file attachments with a meaningful name that will help the recipient to know what the attachment is about without opening it.

4.5. Double-check that the intended attachment is indeed attached to your email before sending.

5. Automatic Replies
   5.1. Configure Automatic Replies to be sent when you plan to not be checking your email for a few days.
   5.2. At a minimum, the automatic reply should specify when you plan to respond to your emails and who to contact if a faster response is required.

Appendix 2 – Email Acceptable Use

1. GPRC staff and faculty are prohibited from using external email accounts (such as Gmail, Hotmail, Yahoo mail, etc.) for business communication, including communication with students.

2. GPRC staff and faculty are prohibited from automatically forwarding GPRC email services to any external email account or messaging service.

3. Flaming (emotional outbursts sent via email or instant messaging), bombing (overloading the network or a specific email / instant messaging account through a deluge of emails) or spamming (sending emails or messages that are unsolicited and in no direct relation to Institution business) are prohibited.

4. Electronic mail and instant messaging are considered open and non-secure communication. Sending confidential information via email and instant messaging without encryption is prohibited. All email communication must follow the Record Classification and Handling Policy.

5. Email signatures must be as specified in section 10.1 of the GPRC Style Guide. Emails sent to external users, students, or clients must contain an email signature.

6. Users are prohibited from accessing another user's email without his or her permission.

7. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their account by unauthorized individuals.