IT ACCEPTABLE USE POLICY

IT ACCEPTABLE USE POLICY			
Effective Date	May 20, 2016	**Cross- Reference**	1. Communication Policy 2. Employee Discipline Policy 3. IT Password Policy 4. IT Email Policy 5. IT Password Policy 6. IT Technology Access Policy 7. Protection of Privacy Policy 8. Record Classification and Handling Policy 9. Student Printing Policy
Responsibility	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. Acceptable Use 2. Unacceptable Use 3. Acknowledgement Form

1. Policy Statement

1.1. Grande Prairie Regional College (“GPRC” or the “Institution”) expects all employees, contractors, students, visitors or volunteers to use information technology, networks and related IT systems in a professional manner.

2. Background

2.1. Information technology provided by the Institution is first and foremost to be used for serving the interests of the Institution, its clients and customers in the course of normal operations.

2.2. All users must follow the acceptable use guidelines and requirements defined in this policy to prevent disruptions to business operations and mitigate unnecessary costs.

3. Policy Objective

3.1. The objective of this policy is to define detailed requirements related to the acceptable and unacceptable use of Institution IT systems.

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, visitors, volunteers and authorized users accessing Institution IT systems and applications.

4.1.3. All IT systems or applications managed by the Institution that are storing, processing or transmitting information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

5. Definitions

5.1. “Users” include students, employees, consultants, contractors, agents and authorized individuals with access to GPRC IT systems and applications.

5.2. “GPRC Network” includes any network that directly accesses GPRC systems without traversing through the GPRC firewall. Networks that only have access to the internet, such as the GPRC public wireless network, are not considered to be part of the GPRC Network in this policy.

6. Guiding Principles

6.1. This policy does not address every possible scenario; users are expected to operate in a manner consistent with the expectations set out in this policy, using reasonable judgment in a manner that supports effective business operations.

6.2. Users must follow the requirements defined in the Communication Policy and the IT Email Policy for the appropriate communication of information.

6.3. Users must follow the requirements defined in the IT Technology Access Policy for the appropriate access to the GPRC IT systems.

6.4. “Confidential” and “Restricted” GPRC information must not be removed from any GPRC location or sent out electronically to an external party without prior approval. Furthermore, such information must be secured and protected while in transit and during use, as required by the Record Classification and Handling Policy. Specifically:

6.4.1. Users must not disclose any Confidential or Restricted information (such as GPRC business, technical or customer information) to third parties without advanced written authorization by the Senior Leadership Team member that is responsible for the information (i.e. Disclosure of employee information requires approval of the Human Resources Director).

6.4.2. Help Desk or the IT Director must be notified immediately when such GPRC collegial business or student information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties. The Help Desk will notify applicable personnel and ensure required processes are followed.

6.5. Users must follow the detailed requirements in **Appendix 1** (Acceptable Use) and **Appendix 2** (Unacceptable Use).

6.6. Users provided with access to GPRC computing systems, applications or resources must agree to the Acceptable Use and IT Policies agreement form (provided electronically to users). A sample of this electronic form is included in **Appendix 3**.

6.7. GPRC reserves the right to monitor, inspect, and/or search at any time all GPRC information systems and devices. This examination may take place with or without the consent, presence, or knowledge of the involved user(s). GPRC additionally retains the right to remove from its information systems any material deemed to be inappropriate or potentially illegal.

6.7.1. This examination can only be conducted as part of an ongoing Human Resources investigation, and must be authorized by the Director, Human Resources.

6.7.2. Any information collected will be considered confidential and provided solely to the Director, Human Resources as part of their internal investigation.

6.7.3. Any information collected will be managed in accordance with the Protection of Privacy Policy, the Record Classification and Handling Policy, and the Records Management Policy.

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. • Review and approve any exception requests relative to the requirements in this policy. • Take proactive steps to reinforce compliance with this policy by all stakeholders.
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 this policy upon the first day of commencing work with GPRC. • Support all employees and students in the understanding of the policy requirements.
All users (Employees and contractors, Students, Visitors and Volunteers)	• Comply with the applicable requirements of this policy at all times. Failure to comply with this policy, may result in disciplinary action as outlined in the Employee Discipline Policy. • Report all instances of non-compliance 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 Vice-President Administration, with evidence of support from the appropriate Vice-President.

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(s)

8.2.4 Evidence of approval by the Vice-President Administration.

9. Inquiries

9.1 Inquiries regarding this policy can be directed to the Information and Privacy Coordinator and/ or the Information Technology Director.

10. Amendments (Revision History)

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

10.2 Post-Implementation Policy Review Approval: January 29, 2019

Appendix 1 – Acceptable Use

1. Use of Computing Equipment

1.1. Users must follow operating procedures and usage guidelines as defined and communicated by the IT department when using Institution IT systems.

1.2. GPRC IT equipment and related hardware and software are the property of the Institution. As such:

1.2.1. Users are responsible for the IT equipment that is attributed to them and must take care of such equipment to prevent any damage.

1.2.2. When users are no longer employed by GPRC, all IT equipment assigned to them must be returned to the Help Desk immediately.

1.3. Users must ensure that computing equipment is always protected against loss or theft, or theft of the information stored on the equipment. This includes:

1.3.1. Not leaving mobile or portable devices (smartphone, laptops, tablets, USB keys or projectors) unattended, even for a short period of time, unless they are appropriately secured.

1.3.2. Attaching unattended laptops to a desk or a secure anchor point using a security cable.

1.3.3. Ensuring that laptops or tablets are secured in a locked cabinet, drawer or office when left unattended.

1.3.4. Reporting all losses immediately to the Help Desk.

1.3.5. Securing unattended IT systems with a password-protected screen saver. The screen saver must be engaged by using the “Windows” + “L” command every time a user leaves a computer unattended, even for a short period of time.

1.4. All changes to GPRC networks and systems must be approved in advance by means of the approved change control process. Changes must only be made by persons who are authorized by the IT Director and/or the Help Desk.

1.5. Only authorised Institution equipment is allowed to be connected to the internal GPRC network environment.

1.6. Access to all GPRC systems and information requires explicit management approval following the IT Technology Access Policy. Such access must be limited to only the systems and information necessary for the role or job description of each user, as intended and formally approved by management. Further:

1.6.1. When an employee, contractor or agent changes responsibilities and duties (including termination, transfer, promotion, leave of absence) the users’ supervisor must notify Help Desk and the Human Resources department on a timely basis.

1.6.2. Each user receives a unique username and password to access information on GPRC computing systems. Users are responsible for the security and usage of their password and account and they must not share their passwords with any third party, including managers, staff, friends, family, or household members. Further, users must not request the password of another user. If a user password is required for troubleshooting or diagnostic purposes, the user must enter the password him/herself.

1.6.3. Users must change their passwords at appropriate intervals in line with the requirements of the Password Policy. Passwords must be changed immediately when there is a concern that the password has been compromised.

1.6.4. Remote access to GPRC computer networks, when approved, must be performed following GPRC requirements, which includes the use of a computer equipped with the latest operating system patches applied, up-to-date antivirus software and a local firewall enabled.

2. Physical Workspace Security

2.1. Access to every office and GPRC work area that contains restricted or confidential information must be physically restricted to those people with approved permission to access these areas. Users must not attempt to access areas where they do not have permission.

2.2. When left unattended, restricted or confidential information, as per the Record Classification and Handling Policy, must be protected from unauthorized disclosure as follows:

2.2.1. Unless restricted or confidential information is in active use by authorized people, desks must be clear and clean of such information.

2.2.2. Restricted or confidential information in paper form must be locked away in appropriate containers (e.g. safes, file cabinets, etc.).

2.3. Computer equipment (that is not designed to be portable) may not be removed from GPRC offices unless the involved person has first obtained written permission from the Help Desk; laptops, tablets and smartphones are not subject to these requirements.

3. Use of Software

3.1. GPRC shall provide licensed copies of software so that users can perform all required Institution related duties. GPRC must make appropriate arrangements with vendors for additional licensed copies, if and when additional copies are needed for business activities. To ensure compatibility with GPRC networks and computers, and to allow licenses to be properly managed and audited, all software must be purchased through the procurement process. The IT Director must be advised in writing when software licenses are purchased through alternate channels.

3.2. The installation of any software not previously approved by the IT Director is prohibited on GPRC computing resources. A formal request to the Help Desk is required when there is a need for installation of any applications not installed as part of the standard system build or on the GPRC list of approved software.

3.3. License agreements for software acquired by GPRC must be respected and users must not copy GPRC licensed software to any storage media, transfer such software to another computer, or provide such software to outside parties without advance permission from the software owner, the vendor or the IT Director, as appropriate. Ordinary back-up copies are an authorized exception to this policy, where permitted by copyright laws.

4. Internet Use

4.1. The use of email must follow the IT Email Policy.

4.2. When sending emails to an external person (i.e. Internet email address) the user must always:

4.2.1. Verify that the content of the email does not contravene the Record Classification and Handling Policy.

4.2.2. Double-check the destination email address to prevent involuntary disclosure of sensitive information.

4.3. Consuming a large volume of data and bandwidth over the Internet, such as streaming online movies, is prohibited, unless an exception has been granted for business reasons.

4.4. The use of the Internet for legitimate business purposes is permitted at all times. Limited personal use of the Internet for non-business purposes is permitted at the supervisors' discretion.

4.5. Users must ensure that their Internet use is appropriate and lawful and complies with the Institution Communication Policy. Specifically, users must not intentionally access websites that are potentially unlawful, insecure or susceptible to interference or disruption to business work.

5. Use of Telephones and Fax Machines

5.1. Long distance calls or fax is not permitted for personal use unless approved by your manager. GPRC personnel may be responsible to repay the Institution for any personal long distance usage incurred on both land and cellular telephones.

6. Use of Printing Resources

6.1. All users must refrain from printing unnecessary documents in order to reduce the Institution impact to the environment and minimize costs.

6.2. Use of printing resources is not permitted for personal use unless approved by your manager. GPRC personnel may be responsible to repay the Institution for any personal printing or photocopying.

6.3. Students must follow the Student Printing Policy.

Appendix 2 – Unacceptable Use

1. It is prohibited to publish the following information by email, instant messaging tools, and social media networks on the Institution Intranet or the Internet in general:
    1.1. GPRC confidential information
    1.2. Information that is defamatory to others or the Institution
    1.3. Information that is considered insulting, aggressive, or of a harassing nature against others or the Institution
    1.4. Information that may be provocative or harmful to others or the Institution
    1.5. Information that is intended for personal gain, political positioning, or social positioning
    1.6. Information that is protected by copyright or intellectual property
    1.7. GPRC Information that has not been formally approved by the Institution for publication
2. Accessing and using GPRC information technology services without authorization is prohibited.
3. Using GPRC information technology infrastructure for illegal activities that contravene the law, regulations or existing Institution policies is prohibited.
4. Any attempt to disrupt the intended use of GPRC system or network resources is prohibited. Use of GPRC information technology infrastructure that is contrary to the intended purpose of the systems and applications, as interpreted by management, or that serves a personal benefit that is contrary to the Institution benefits or interests is prohibited.
5. Attempts to read another person's information unless otherwise authorized is prohibited. Further, any intentional activity that results in the damage to GPRC files, equipment, software or data belonging to others is prohibited.
6. Attempts to circumvent any controls put in place to protect information technology assets is prohibited. Specifically:
    6.1. Bypassing or trying to bypass user authentication or security of any computer system, network or account to gain information or access is prohibited.
    6.2. The purposeful or neglectful introduction of malicious software, executable code or scripts (including but not limited to: viruses, worms, Trojan horses, e-mail bombs, exploits, etc.) into the network or server environments is prohibited.
    6.3. Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the IT Director. Testing of any GPRC owned hardware or software is only to be performed by individuals with a job role requirement to perform such testing.
    6.4. Unless specifically authorized by the IT Director, GPRC users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security.
    6.5. Causing a loss of service to any computer system or communications device is prohibited.
7. Users are prohibited from connecting personal equipment or adding non-approved computing devices (portable or fixed) to the GPRC network and systems unless formally and explicitly approved by the IT Director.

8. The installation of the following technologies can only be performed with a formal approval from the IT Director:
   8.1. Modems for in-bound or outbound dial-in purposes
   8.2. Wireless access points
   8.3. Remote access software such as LogMeIn, TeamViewer, any VNC, Radmin, Citrix, etc.
   8.4. Peer-to-peer file sharing
   8.5. “Cloud-based” solutions, such as “Dropbox”, online “CRM tools”, or any other Software as a Service (SaaS)

Appendix 3 – Acknowledgement form

I acknowledge that I have received, read and fully understand the following policies, their content, requirements and expectations. I agree to abide to these policies, their content, requirements and expectations as a condition of my continuing employment or contract with the Institution. I understand that I am personally responsible for compliance with these policies:

- IT Acceptable Use Policy
- IT Password Policy
- Record Classification and Handling Policy
- IT Communication Policy
- IT Email Policy
- Protection of Privacy Policy
- IT Technology Access Policy

I acknowledge that the Institution may alter the existing policies from time-to-time and that any such changes will be communicated through formal communication. Once notified, I will read, understand and abide to the updated policies.

I understand that if I have questions on these policies, I will immediately consult with my immediate supervisor or the Human Resources Department.

Signature

Date

First and Last Name