# IT TECHNOLOGY ACCESS POLICY

| IT TECHNOLOGY ACCESS POLICY | | | |
|---|---|---|---|
| **Effective Date** | May 19, 2016 | **Policy Type** | Administrative |
| **Responsibility** | Director, Information Technology | | |
| **Approver** | Executive Council | **Cross- Reference** | 1. IT Access Control and User Access Management Policy<br>2. IT Acceptable Use Policy |
| **Review Schedule** | Every 5 years | **Appendices** | 1. Access to IT Systems |

## 1. Policy Statement

1.1 Grande Prairie Regional College ("GPRC" or the "Institution") requires its students, employees, consultants, contractors, visitors, volunteers and users to follow a formal process when requesting access to, and using technology equipment, hardware and software.

## 2. Background

2.1 The Institution invests in technology systems for business purposes that are expensive to acquire and maintain. To prevent cost overrun and inappropriate usage, access to IT systems are provisioned to authorized users based on business needs.

## 3. Policy Objective

3.1 The objective of this policy is to define requirements related to the use of, and access to Information Technology (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 users accessing Institution IT systems and applications.

4.1.3 All IT systems or applications managed by the Institution, or by a third party on behalf of 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 "Guest users" are non-permanent employees or contractors that are granted temporary access to some GPRC IT systems and applications.

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

## 6. Guiding Principles

6.1 Access rights provisioned to IT systems and applications must follow the IT Access Control and User Access Management Policy.

6.2 When users are accessing IT systems, they must follow the IT Acceptable Use Policy at all times.

6.3 Requests to access Institution IT systems or to obtain a new IT system must be submitted to Help Desk and must be formally approved by the supervisor. Additional information is included in Appendix 1.

6.4 In the event of detection of system access which violates Institution policies and standards, GPRC will contact the user, their manager, supervisor and Human Resources (HR) as applicable. The Institution reserves the right to immediately remove access or disconnect any unauthorized equipment.

6.5 All users must follow the detailed requirements in Appendix 1.

## 7. Roles and Responsibilities

| Stakeholder | Responsibilities |
|---|---|
| Executive Council | • Approve and formally support this policy. |
| Vice President, Administration | • Review and formally support this policy. |
| Director, Information Technology | • Develop and maintain this policy.<br>• Take proactive steps to reinforce compliance with this policy for all stakeholders.<br>• Review and approve any exception requests relative to the requirements in this policy. |
| Institution Management, Supervisors or Representatives | • Explain the terms of this policy to employees and students and assist the users in the understanding of the requirements of this policy.<br>• Ensure that all users follow the requirements of this policy. |
| Contract Administrators and Managers | • Follow the guidelines provided in this policy to perform due diligence and assess the risks related to security for any new contract.<br>• Ensure that the 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 with GPRC.<br>• Support all employees and students in the understanding of the requirements of this policy. |
| All users (Employees and contractors, Students, Visitors and or Volunteers) | • Comply with the requirements of this policy.<br>• 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.

8.2 Policy exceptions must describe:

8.2.1 The nature of the exception

8.2.2 A reasonable explanation for why the policy exceptions are required

8.2.3 Any risk created by the exceptions to this policy

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 Review: Approved March 5, 2019

## Appendix 1 – Access to IT Systems

### 1. Local and Remote Access to the Network

1.1. Access to the Institution network domain must be granted following the IT Access Control and User Access Management Policy.

1.2. The following requests must be formally approved by the IT Director, or designate:

1.2.1. Connection of any non-Institution system to the Network.

1.2.2. Usage of any non-standard remote access solutions, including VPN connections and remote connection tools such as “Remote Desktop”, “LogmeIn”, “TeamViewer”, “VNC” or “GotomyPC”.

1.2.3. Connection of ad-hoc Wi-Fi access points (AP) or dial-up modems.

### 2. Access to Wi-Fi Networks

2.1. GPRC may provide access to a Wi-Fi network for the convenience of guest users to access the Internet. The connection of equipment to this “guest” Wi-Fi network is permitted under the following conditions:

2.1.1. Access to the “guest” Wi-Fi network requires a password (also referred to as a pre-shared key – PSK) that is changed regularly.

2.1.2. Access to the “guest” Wi-Fi network requires acceptance of the displayed terms and conditions.

2.2. GPRC may provide a Wi-Fi network for GPRC users to access the internet. This “users” connection to this Wi-Fi network is strictly reserved to GPRC authorized users.

2.3. GPRC may provide a Wi-Fi network for users to access the internal network. The connection to this “internal” Wi-Fi network is strictly reserved to GPRC authorized users with GPRC equipment.

2.4. Non-GPRC devices such as employee owned smartphones, laptops, or tablets must not be connected to the GPRC internal network unless approval is formally obtained from the IT Director. These devices can be connected via the “guest” or “users” Wi-Fi networks.

### 3. Access to GPRC Equipment

3.1. The IT Director reserves the right to immediately remove access, disconnect or repossess any equipment.

3.2. When an appropriate business requirement supports the need for a user to be granted a GPRC laptop or tablet, a formal request must be sent to the Help Desk. The request must be formally approved by a manager / supervisor.

3.3. When an appropriate business requirement supports the need for a user to be granted a GPRC mobile phone (cellular / smartphone), a formal request must be sent to the Help Desk. The request must be formally approved by a dean / director.

3.4. Laptops, tablets and mobile phones are provided to GPRC employees and contractors based on the job role and responsibilities, at the discretion of the IT Director.

## 4. Access to GPRC Mobile Phones

4.1. The following criteria will be used to determine an employee's need for a mobile phone:

4.1.1. Safety requirements indicate having a cell phone is essential to fulfilling job responsibilities.

4.1.2. More than 50% of work is conducted off-campus or away from the regular workplace including, but not limited to the employee's office, classroom, lab or shop.

4.1.3. The employee is required to be available and responsive on a regular basis outside normal work hours.

4.1.4. Job requirements include critical College-wide decision making and/or incident response duties.

4.2. GPRC mobile phones must stay operational during normal working hours so employees can be reached and have easy access to their email and calendar.

4.3. GPRC mobile phone numbers are published and available to all College staff and are not considered personal information.

4.4. Devices with GPRC mobile phones numbers are to be primarily used for business calls, Institution emails and calendar systems. Reasonable access to the Internet for business is allowed. All other usage that is not directly related to GPRC work must be kept to a minimum as additional costs may be incurred or specific cyber risks can be encountered.

4.5. Employees that qualify for a GPRC mobile phone can choose to:

4.5.1. Be provided a GPRC mobile phone with a GPRC mobile phone number.

4.5.1.1. IT will select a small number of available devices for use as GPRC mobile phones. Only these pre-selected devices will be provided by GPRC.

4.5.2. Purchase their own device, and have a GPRC mobile phone number assigned.

4.5.2.1. Employees are responsible for purchasing their own devices.

4.5.3. Receive $40/month towards a device and the related monthly expenses to use as their GPRC mobile phone.

4.5.3.1. No additional reimbursements will be provided.

4.5.3.2. Employees are responsible for purchasing their own devices.

4.5.3.3. Phone numbers of these devices will be published in the same manner as GPRC mobile phone numbers.

4.6. Infrequent or moderate use of a personal cell phone for College business is considered normal and will not be reimbursed. If an employee is not eligible for a College provided cell phone, he/she may request reimbursement only to the extent that additional expenses were incurred. The individual should make personal payment to the provider, and then submit a request for reimbursement to Finance, along with a copy of the cell phone bill. When possible, business calls while on campus should be made from traditional landline phones.

4.7. If deemed un-reasonable, the following costs associated with a GPRC mobile phone or tablet may be charged to the user:

4.7.1. Costs associated with installed applications and programs

4.7.2. Repairs and maintenance costs beyond the costs covered by the normal warranty

4.7.3. Personal long distance costs

4.7.4. Excessive data usage costs, including data roaming charges incurred while outside Canada for non-related GPRC business

4.7.5. Any other costs incurred that have not been approved

4.8. GPRC smartphones and tablets, and personal devices that are used to access GPRC Active Sync for employee account, are to be enrolled with the Institution Mobile Device Management (MDM) server. The MDM system enforces the use of a passcode on smartphones and tablets.

4.9. When they are locked, GPRC mobile devices, and personal devices that are used to access GPRC Active Sync for employee account, must display a phone number that can be used as a point of contact by any person who finds the device in the unfortunate event of a loss.

4.10. Apps for GPRC mobile devices must only be downloaded and installed from trusted sources such as the Microsoft store, Blackberry store, Google Play store and the Apple store. It is prohibited to obtain apps from other sources as they present a security risk (e.g. phishing apps, apps that can spread malware, apps that can automatically download the user’s personal information or any sensitive information from the device).

Further, the user must not install “apps” that:

4.10.1. May incur additional service costs

4.10.2. Negatively impact the performance of the device