

CITY OF CHESTERMERE

POLICY HANDBOOK

EFFECTIVE DATE: May 22, 2018		SECTION: 800	POLICY: 836
APPROVED BY: Council	APPROVED DATE: May 22, 2018	TITLE OF POLICY: Information Technology (IT) End User Policy	
REVIEW DATE: January 2020	AMENDMENT DATE: N/A	PAGE NO.: 1 of 14	
POLICIES AMENDED / RESCINDED: Policy 728 – Computer Use		POLICY TYPE: Council	

PURPOSE

The purpose of this Policy is to provide users with general guidelines for the appropriate use of the City of Chestermere's Information Technology End User Resources. This Policy will help the City maintain control, stability and security of its Information Technology Resources. It will facilitate equitable and position-appropriate allocation of these resources to support the most efficient and effective use of technology in carrying out City business.

DEFINITIONS

- a. Appropriate – refers to uses that are professional, responsible, not harmful and bona fide, that promote and assist the User in his/her job duties and are aligned with the City's Vision, Mission, Values and Strategic Principles.
- b. BYOD – Bring Your Own Device; any device that is not owned by the City.
- c. City – the City of Chestermere in the province of Alberta.
- d. Contractor – an independent party (person, business or corporation) which provides goods or services to the City under terms specified in a contract.
- e. Councillor – an elected official of the City of Chestermere.
- f. Data – facts or figures, or information that is stored electronically or originating in other forms.
- g. Employee – any individual currently employed by the City, including permanent full-time, permanent part-time, casual, temporary, probationary, student or paid or unpaid volunteer personnel.

81

- h. FOIP Act - *Freedom of Information and Protection of Privacy Act* – the Act that protects an individual's privacy by setting out rules for collection, use or disclosure of personal information by public bodies.
- i. Hardware – tangible computer resources such as desktop computers, laptops, tablets, internet accessible devices, telecommunications equipment (including cellular devices), printers, photocopiers and all related network infrastructure.
- j. Information Technology (IT) Function Area – includes the personnel and Contractors assigned the authority to manage and administer the City's Information Technology Resources.
- k. Information Technology (IT) Resources – includes but is not limited to computing, networking, communications and telecommunications systems, infrastructure, Hardware, Software, data, databases, personnel, procedures, physical facilities, and any related materials and services, owned and managed by the City.
- l. Internet – a matrix of networks that connect computers around the world.
- m. Intranet – private network for Chestermere employees to use for information available through the Chestermere website.
- n. LAN – Local Area Network, the private network that the city of Chestermere used for all data connections
- o. Records – the representation of or a record of any information, data or other thing that is or is capable of being represented or reproduced visually or by sound, or both, including but not limited to correspondence, data, databases, documents, emails, files, images, photographs, reports and spreadsheets.
- p. Software – non-tangible computer resources such as computer operating systems and computer programs.
- q. Subscriber Identification Module (SIM Card) – an integrated circuit that is intended to securely store the international mobile subscriber key and data for cellular telephone subscribers.
- r. Supervisor – the employee's direct supervisor, as named in the employee's job description, or the City employee to whom a Contractor or volunteer reports while engaged on behalf of the City.
- s. User – user of the City's Information Technology Resources that may be either Employee, Contractor, Councillor, or other individual authorized by the City to access the IT Resources.
- t. Visitor – any individual who attends any City building, facility, event for business or entertainment purposes.

- u. WAN – Wide area Network, network outside of the LAN, the internet.
- v. Wireless Fidelity (WiFi) – is a technology for wireless local area networking.
- w. Work Shift – the hours the employee is on paid duty working for the City or whenever the Contractor or volunteer is acting on behalf of the City.

POLICY STATEMENT

It is the policy of the City of Chestermere that Appropriate, secure and functional access to corporate information and technology is provided to those who require it for the purpose of carrying out City business in an effective and efficient manner. To ensure Appropriate use of corporate information and technology, Administration will develop policies and procedures to meet operational and legislative requirements. All City IT Resources Users will be required to complete and sign an Information Technology End User Policy Acknowledgement and Use of IT Resources Agreement (Appendix 1).

This Policy does not apply to two-way radio use.

RESPONSIBILITIES

Link to City's Vision, Mission and Strategic Principles

The City actively pursues opportunities to create innovation in its IT Resources and practices while balancing risk and fiscal responsibility.

Application

This Policy applies to all City Councillors, Employees, Contractors, and Visitors utilizing City IT Resources.

Ownership

All computers, printers, Data, electronic documents, Records, images, files, internet addresses, internet correspondence, and operating Software, whether or not such items are assigned for the specific or general use of an User, are owned by the City.

The City owns (i) all Records that are received, generated, or maintained by any Councillor, officer, employee or consultant in the course of carrying on City business or providing City Services, regardless of whether the Record was generated on City or non-City computers, received or sent on City or non-City internet email accounts or created using City or non-City Software, (ii) all Records that are maintained on the City's hardware, and (iii) all Records that are received by the City from any Visitor.

All intellectual property created using City equipment and/or Software and/or Data shall remain the property of the City

The IT Resources to be allocated to each User based on the needs of their position, as outlined by Human Resources, and as approved by their Director in collaboration with the IT Function Area. The IT Function Area personnel may from time to time access the User's equipment or devices. Access will be determined either at the sole discretion of the Chief Administrative Officer or through a request from an IT Function Area personnel. If requested through IT, full cooperation is expected and any such request will not be unreasonably withheld by the User.

All IT costs will be budgeted within the IT Function Area but tracked by each respective Department and Function Area within the IT budget.

The City does not support BYOD or the use of user-owned devices by Users. Any exceptions will be dealt with on a case-by-case basis with authorization specifically provided by the Chief Administrative Officer.

Access

Each User is provided with the use of a Hardware and access to the City's network and information system. It is important that each User understands the responsibilities with respect to the Hardware and system:

a. Hardware

- i. Moving Hardware or other peripheral devices is not permitted without prior approval and/or the assistance of the IT Function Area.
- ii. Connecting unauthorized equipment to any City Hardware or network is prohibited.
- iii. All Users are responsible for the safekeeping, care and cleanliness of the IT Resources used by them.

b. Printers

- i. The City's printer/copier/scanner/facsimile assets are connected through the City's network via the print-server system. This system provides each user with an access code to retrieve print jobs and access copier/fax/scanner services, reducing waste and maintaining confidentiality of documents within the organization.

Employees may use assigned or unassigned computers, assigned internet email accounts, and operate Software to perform the duties and responsibilities assigned to them or to practice or complete homework for courses being taken as required or provisioned for by their position as approved by their Director.

File Storage and Back-up

Users shall store all business-related files on the City's network.

Daily backups of the City's network are automated and retained. Access to or recovery of any stored data or files will be coordinated through the City's IT Function Area.



Each User is assigned a personal drive and all Users have access to a shared global drive and specific functional folders in accordance with the requirement of their position and level of authority in the organization. It is the responsibility of the individual User to manage the storage and retention of digital data in alignment with the City's Records Retention Policy. Individual User drive space limits may be imposed at any time.

The City is not responsible for personal data stored on the network or local Hardware. All personal data stored on the network is subject to FOIP legislation.

Email

Each User is provided with an email account. Any email sent or received by a User for the purpose of carrying out City Business or using the User's City email account becomes the property of the City. Email is a valuable resource designed to enhance User productivity.

Use of email does impose risk to the City and therefore, it is important that each User understands his/her responsibilities with respect to the system.

All Users are encouraged to regularly review and purge old e-mail correspondence in order to keep the system operating in an efficient and robust manner.

Users shall not forward City emails to a personal email account. Rather, the recommended best practice is for Users to access email through the Office 365 platform when away from their City computer system.

Users shall not create a copy of the City email account.

Users shall not access personal email accounts via City computer systems (ie: through Shaw webmail, Telus webmail, Yahoo email, etc.). Users have the ability to access personal email accounts via their City supplied or personal mobile devices.

Access to City emails may be made via public computers through the Office 365 platform (this would be applicable if a User were accessing email while in a hotel for a conference or other public access computer such as at a library).

Litigation holds will be applied to the emails of any User whose employment or contract is terminated (voluntarily or not) pending any FOIP requests that may be imposed on the City. A litigation hold will be placed on each Council member's email for the duration of their Council term plus two years.

Mobile Phones (cellular, smart)

Mobile phones will be allocated to Users based on the needs of their position, as outlined by Human Resources in the job description, and as approved by their Director in collaboration with the IT Function Area. The City will provide a data plan Appropriate for the needs for each position.

The options for assignment of mobile devices are:

- a. Dual SIM Card City-owned mobile device – Users may be assigned a City-owned mobile phone with the option of using a City-owned phone exclusively for City business or the phone will be furnished with dual SIM cards, where possible, allowing both business and personal use on the same phone. This option is not available for those Users requiring a more durable mobile device. The City will pay for the device and City SIM Card and the User will be required to pay for the User SIM Card.
- b. Single SIM Card City-owned mobile device – the City may issue a single SIM Card mobile. The City will pay for the device and City SIM Card.
- c. User-owned mobile device used for City business – the User is not deemed to require a mobile device as a requirement of their position with the City but chooses to supply their own phone for use with City business. Users will pay the full cost of such device. Employees may access the Government of Alberta purchasing program in which the City participates for the purchase of an Employee-owned mobile device (See Appendix 2). While phones purchased through this plan will remain the property of any Employee/family member, the plans offered through this program are only available to Employees while employed by the City.
- d. No mobile device – the User's position may not require a mobile device and in this situation, the User may choose not to carry a mobile device. The User may also choose to not participate in the Government of Alberta purchasing program.

Users shall not tamper with or remove the City-owned SIM cards from their City-owned mobile phone.

All Users are responsible for the safekeeping, care and cleanliness of the mobile phone(s) they are issued. It is mandatory to activate one of the following:

- i. biometric identity sensor,
- ii. password, or
- iii. personal identification number

to secure the mobile phone and enable the auto-lock feature on the mobile phone. Any use of biometric identity sensor must be accompanied by a password or personal identification number as an alternate method of security.

Upon request the holder of a City-owned SIM card or City-owned mobile phone must provide the password for said device.

All City-owned SIM cards or City-owned mobile phones will be loaded with remote software that wipes the equipment clean. Chief Administrative Officer has the sole discretion as to when such an action would occur or at the end of any Users term of employment or contract. IT has the sole responsibility of activating this software.

BYOD mobile phones, when used for City purposes, will be loaded with remote software that wipes only corporate data clean. Chief Administrative Officer has the sole discretion

as to when such an action would occur or at the end of any Users term of employment or contract. IT has the sole responsibility of activating this software.

The owner of a BYOD will be given the opportunity to request locating, locking and/or wiping clean in part or fully, a lost or stolen device.

Each User will be allowed a one-time, no questions asked replacement of City-owned mobile phone device.

Users shall not call-forward the City's telephone to a personal phone/phone number.

The City participates in a purchasing program in partnership with the Government of Alberta to provide lower cost mobile phone equipment and contracts. These benefits have been extended to City Employees and their families. Detailed information regarding this program may be found in Appendix 2 of this Policy. It is at the sole discretion of the City to change or rescind this program, at any time, without notice.

Additions and Modifications to IT Resources

Users shall not install or connect any unauthorized Hardware or Software on a City workstation or the network. This includes such items as VPN (Virtual Private Network), additional routers, switches, etc.

The City's IT Function Area is responsible for installation, deletion, connection, management and maintenance of City-owned Hardware and Software. All requests related to Hardware or Software connection, installation, system requirements, management and maintenance are to be directed to the City's IT Function Area personnel.

All Software licensing agreements are observed and maintained by the IT Function Area. The City will only install and use legal copies of Software acquired through the IT Function Area. In no case shall private-owned or unauthorized Software be installed, loaded, and/or used on City computer systems

All copyrights and Software licenses and the rules governing such copyrights and Software licenses are to be respected and will be recorded for administrative purposes by the IT Function Area.

Users shall not intentionally install or retransmit any malware, virus or spam using City IT Resources.

Users must consult with the City's IT Function Area if there are questions regarding the use of City licensed Software for legitimate work-related instances at home. Use of Software at home for work-related causes may be acceptable determinant upon the licensing agreement for said Software.

Software audits will take place on a periodic random basis by the City's IT Function Area personnel. All Users must fully cooperate during audit procedures.

IT Help Desk Request for Assistance

The IT Help Desk will provide support to any problems or requests related to the City's Hardware including new purchases of equipment or software. A Help Desk Ticket request must be submitted to IT for each request and can be done through the City's intranet. Each Help Desk Ticket will be reviewed by the IT Function Area and will be responded to in priority sequence.

It is the intent of the IT Help Desk to respond to all Help Desk Tickets within one business day outlining an expected resolution time. The goal is to resolve the majority of Help Desk Tickets within one business day and any Tickets requiring a longer resolution will be identified with an estimated time of completion.

IT Project Implementation Process

There will be a triage process for any new IT Project implementation. The IT Function Area will determine how and when a new IT Project will be implemented and schedule the project within the IT Function Area's work plan. Once the IT Function Area work plan is approved by the Director of Corporate Services, any future change orders to IT Projects will require the approval of the Corporate Leadership Team.

Internet

Access to City provided Internet services are a privilege that may be wholly or partially restricted by the City without prior notice and without the consent of the User.

There are three options for accessing the City's WiFi:

- a. Cityguest – this WiFi connection is available for public to access the City's WiFi while in any City office (City Hall, City Public Works Facility, and City Protective Services Facility). This does not access the City's network and has a 24 hour service limit.
- b. Citymobile – this WiFi connection is available for Users to access the City's WiFi using personally-owned devices while in any City office (City Hall, City Public Works Facility, and City Protective Services Facility). This does not access the City's network.
- c. Chestermere – this WiFi connection is reserved for City-owned equipment and devices with full access to the City's network.

All Internet address, email address, or network account assigned by the City to Users are the property of the City. The use of aliases must be approved by the User supervisor. All aliases must be provided to IT and it will be the responsibility of IT to setup.

Users of City IT Resources, whether such equipment is assigned or non-assigned, shall not access the Internet or email services for websites, information, or images that are not Appropriate (the following is provided as examples and it is not intended to be considered an exhaustive list: hateful, pornographic, obscene, bigoted, racist, sexist or that contain

other offensive materials). Further, Users shall not incite, share or promote messages, websites, information or images that are not Appropriate. Determination of these circumstances shall be at the sole discretion of City management.

Users shall not use electronic communications, whether by email, telephone, fax, network, or other methods, to send, receive, or view fraudulent, unlawful, harassing or obscene messages, images or other materials. Determination of these circumstances shall be at the sole discretion of City management.

Information that is of a sensitive nature or is classified as personal and/or confidential must not be exchanged via the Internet, as the Internet is an open, non-secure data carrier. Please also refer to Social Media Policy #124.

User access to the internet is permitted for personal improvement during lunch, breaks, or after hours, while adhering to the professional conduct of the City and must not be within public view.

Internet Chat channels or other internet forums shall not be used through City IT Resources. Users may access webinar communication in accordance with this Policy. It is advised that Users confirm connection requirements sufficiently ahead of the webinar date/time. Should the IT Function Area not be able to confirm the security of the software, the User may be required to use an IT-supplied, locked computer for this purpose. Users may access the City Skype account for skype communications in accordance with this Policy.

Security

Each User will be provided with a User login and password, which will allow access to the network. User login and passwords are not to be shared with anyone. Each User is accountable for all actions performed with their User login.

Misuse of data, especially for personal gain, will be regarded in the same manner as other types of theft and fraud. A User shall not access data without proper authorization and must not use the network to make unauthorized entry to other information systems.

Upon termination of employment, contract or term, the User must return all City computer property in their possession. The Human Resources Department will advise the IT Function Area when a User leaves the City.

Passwords are used for various security purposes at the City. Some of the more common uses include User level accounts, web accounts, email accounts, and voicemail password. Passwords must follow the prescribed format and guidelines and are not to be recorded or displayed in any location that is easily viewed or accessible by anyone.

Users are expected to secure their Hardware if they are leaving it unattended for any length of time.

Users are expected to shut down or restart their Hardware each night or at the end of your Work Shift, unless otherwise instructed by the IT Function Area.

Privacy and FOIP Act

Users do not have any expectation of privacy with respect to activities conducted and documents stored on the City network, Hardware, City WiFi connection, or other devices and are required to comply with the FOIP Act. In order to protect the City and prevent liability, information received, generated or stored on the City network, Hardware or other devices may be examined, inspected, monitored or reviewed by the City at any time without the User's consent or notification, however this shall be conducted only through specific direction of Council or the Chief Administrative Officer.

All data, received, generated or sent on or through the City's network, Hardware or other devices may be subject to discovery proceedings in legal actions and Freedom of Information and Protection of Privacy Act (FOIP) inquiries.

Personal Use

Personal use is defined as using any City Hardware for any purpose other than those directly related to or required by a User's position.

If an individual uses assigned or unassigned City Hardware at home for City or personal use, the requirements as outlined in this Policy will still apply.

Unless otherwise authorized, City Hardware shall not be used for personal reasons during business hours or during an employee's Work Shift.

Employees may use City Hardware for strictly personal reasons after business hours, during lunch, breaks, or prior to and after their Work Shift; as long as such personal activities do not contravene the guidelines established for personal use of Hardware, as outlined below, and such use does not interfere with the official use of the Hardware by another employee.

- a. The following activities are considered acceptable uses of Hardware for personal use reasons:
 - i. Creating a document, spreadsheet, and database file;
 - ii. Printing personal documents, in small quantities;
 - iii. Using on-line tutorials;
 - iv. Administrative tasks associated with various City User groups, committees, or associations;
 - v. Using City owned Software to enhance one's computer skills and knowledge;
 - vi. Writing e-mails addressed to non-business related persons; and
 - vii. Browsing the internet.

- b. The following activities are not acceptable uses of Hardware for personal use reasons:
 - i. The purposes of compensation or remuneration for or from outside persons or agencies;
 - ii. Development of computer applications with the subsequent use thereof for outside persons or agencies;

Privacy and FOIP Act

Users do not have any expectation of privacy with respect to activities conducted and documents stored on the City network, Hardware, City WiFi connection, or other devices and are required to comply with the FOIP Act. In order to protect the City and prevent liability, information received, generated or stored on the City network, Hardware or other devices may be examined, inspected, monitored or reviewed by the City at any time without the User's consent or notification, however this shall be conducted only through specific direction of Council or the Chief Administrative Officer.

All data, received, generated or sent on or through the City's network, Hardware or other devices may be subject to discovery proceedings in legal actions and Freedom of Information and Protection of Privacy Act (FOIP) inquiries.

Personal Use

Personal use is defined as using any City Hardware for any purpose other than those directly related to or required by a User's position.

If an individual uses assigned or unassigned City Hardware at home for City or personal use, the requirements as outlined in this Policy will still apply.

Unless otherwise authorized, City Hardware shall not be used for personal reasons during business hours or during an employee's Work Shift.

Employees may use City Hardware for strictly personal reasons after business hours, during lunch, breaks, or prior to and after their Work Shift; as long as such personal activities do not contravene the guidelines established for personal use of Hardware, as outlined below, and such use does not interfere with the official use of the Hardware by another employee.

a. The following activities are considered acceptable uses of Hardware for personal use reasons:

- i. Creating a document, spreadsheet, and database file;
- ii. Printing personal documents, in small quantities;
- iii. Using on-line tutorials;
- iv. Administrative tasks associated with various City User groups, committees, or associations;
- v. Using City owned Software to enhance one's computer skills and knowledge;
- vi. Writing e-mails addressed to non-business related persons; and
- vii. Browsing the internet.

b. The following activities are not acceptable uses of Hardware for personal use reasons:

- i. The purposes of compensation or remuneration for or from outside persons or agencies;
- ii. Development of computer applications with the subsequent use thereof for outside persons or agencies;

- iii. Installing Software without authorization from the IT Function Area;
- iv. Copying City data;
- v. Copying City program files;
- vi. Accessing or downloading files of an inappropriate nature from the internet as noted in the "Internet" section of this Policy;

Failure to Comply

It is each User's responsibility to be familiar, and comply with this Policy. Supervisors, Managers and Directors are responsible for ensuring all Users comply with this Policy.

All reports of alleged inappropriate use of City IT Resources will be reviewed on a case by case basis, by the IT Function Area and reported to the Human Resources Department and/or Chief Administrative Officer of the City, if deemed necessary.

Employees, Contractors or Volunteers found to be in non-compliance with this Policy will be subject to appropriate disciplinary action, up to and including dismissal. Elected Officials found to be in non-compliance with this Policy will be subject to the appropriate disciplinary action as outlined in the Elected Officials Code of Conduct Bylaw #022-17.

Confirmed incidents of blatant misuse involving hate, pornographic, bigoted, or racist sites will result in immediate dismissal from employment with the City.

Determination of these circumstances shall be at the sole discretion of the City.

REFERENCES

- Records Management Policy #719
- Social Media Policy #124
- Employee Code of Conduct Policy #736
- Elected Officials Code of Conduct Bylaw #022-17

For Council Policies:

Approved by Council: *May 22, 2018*



Mayor

Approved by CAO:



CAO

APPENDIX 1 - Information Technology End User Policy Acknowledgement and Use of IT Resources Agreement - City of Chestermere Council Policy #836

Name of User _____ Department _____

The purpose of this Acknowledgement and Agreement is for each User to acknowledge the awareness and understanding of Council Policy #836 – Information Technology (IT) End User Policy and to agree to the terms of use of all applicable IT Resources as defined within this Policy.

I have been assigned a City-owned mobile device with a single SIM Card Yes No

I have been assigned a City-owned mobile device with a dual SIM Card Yes No

I use a personally-owned mobile device for City business Yes No

Personal mobile phone number that may be published (required): _____

I have been assigned other City-owned device(s) Yes No

I will only be accessing City email via Outlook Web Access or Microsoft Online Portals Yes No

The User acknowledges that use of a City-owned mobile device with single or dual SIM Cards or a personally-owned mobile device for City business purposes are ALL subject to the FOIP legislation and that the City will take appropriate measures to protect the liability of the City with regard to the security of any of the above-mentioned devices.

The User must notify the IT Function Area immediately upon knowledge of a mobile device security breach (ie: if a mobile device, either City-owned or personally-owned for City business use, is discovered missing, lost or stolen).

To manage the security of all mobile devices used for City business, the City's IT Function Area will use IT management software that can control the security of a mobile device and/or the data related to a mobile device by remote access. Depending on the security threat determined by the IT Function Area, various security measures may be taken upon the notification by a User of a mobile device security breach, including erasure of data from the device.

By signing this Acknowledgement and Agreement, I _____:

Have read and understand Council Policy #836 – Information Technology (IT) End User Policy and agree to comply with the terms and conditions contained in the document.

Agree to the use of IT management software and activation of this software on the mobile device(s) I use for City business purposes.

Agree to refrain from transferring City email and data to personal email accounts.

Agree to refrain from forwarding City phone calls to personal phone numbers.

User Signature

Date

Name of Supervisor/Manager/Director

Signature of Supervisor/Manager/Director

Date

This form will be reviewed and signed by the User: 1) at time of employment, start of contract, 2) at time of each annual performance review or for Council, at each annual organizational meeting

APPENDIX 2 – GOVERNMENT OF ALBERTA CORPORATE CELL PLAN

Government of Alberta Approved Affiliates

Special offer for employees: Month-to-month network contract

Please note: a price cap is not service cap. Users continue to use these services each month, paying the capped pricing amount when the cap has been met or extended. Please review the acceptable use policy below for details on acceptable use.



	PCS VOICE OFFER	BLACKBERRY AND SMARTPHONE / IPHONE VOICE AND DATA OFFER
Base Charge	\$2/month	\$7/month
Weekday minutes	\$0.01/min for the first 1000 minutes Monthly price cap of \$10 — no charge for minutes beyond the first 1,000.	
Unlimited evenings/weekends from 6pm	\$2/month	
Canada-to-Canada long distance	\$0.02/min for the first 250 minutes Monthly price cap of \$5 — no charge for minutes beyond the first 250.	
Canada-to-U.S. long distance	\$0.04/min for the first 250 minutes Monthly price cap of \$10 — no charge for minutes beyond the first 250.	
U.S.-to-Canada/U.S. long distance	\$0.10/min for the first 100 minutes Monthly price cap of \$10 — no charge for minutes beyond the first 100.	
U.S. voice roaming	U.S.-to-Canada/U.S. long distance rate plus \$0.10/min No price cap.	
SMS within Canada	\$0.02/message for first 125 outgoing messages. Monthly price cap of \$2.50 — no charge for messages beyond the first 125. No charge for incoming SMS messages.	
MMS picture and video messaging	\$0.25/message No price cap.	
SMS within the U.S.	\$0.05/message for the first 100 outgoing messages Monthly price cap of \$5 — no charge for messages beyond the first 100. No charge for incoming SMS messages.	
Data usage within Canada	N/A	\$0.03/MB for the first 667 MB Monthly price cap of \$30 — no charge for data beyond the first 667 MB.*
Data usage within the U.S.		\$0.15/MB No price cap.
Directory Assistance (411)	\$2.50/call	
Included features	Call display, call waiting, call forwarding, conference calling, voicemail.	

*Up to a maximum of 3 GB. Under the acceptable use policy for this offer, TELUS considers 3 GB of data per month to be the acceptable usage allowance.

For hardware details or to apply for this offer, contact one of the TELUS Authorized Dealer(s) listed below.

For information on these rate plan offers, contact **Anne Reyes** at anne.reyes@telus.com



Government of Alberta Approved Affiliates Employee Offer

The **Government of Alberta (GoA) Approved Affiliates** Employee Purchase Program (EPP) offer is intended for use as a wireless service. The user should not swap the SIM assigned to this offer to an alternative device nor use the service for alternative purposes such as ADSL, tethering or large data consumption services. Users proven to be using the service for non-EPP intended use may lose access to this offer. TELUS Acceptable Use policies may be viewed at telus.com/aup.

The GoA Approved Affiliates Employee pricing offers employees preferred pricing plans, features, discounts and select hardware for voice and smartphone use.

- **This Employee offer is limited to one offer per employee.** An employee is eligible to have one EPP plan for either a) voice device or b) voice & data device. Account must be registered under employee name and billed to the employee's address.
- Employees who terminate their employment with the company will no longer be eligible for this EPP offer and are required to migrate to an in-market Consumer price plan on a Consumer BAN. TELUS has the right to contact an EPP user during the annual EPP review, if determined they are no longer employed with the GoA Approved Affiliates and are still operating under the EPP program, they will be requested to move to an alternative Consumer offer.
- Users must produce their employee ID card and a current pay stub for access to the GoA Approved Affiliates EPP offer, NO other forms of identification will be accepted.
- Employees must meet the TELUS credit requirements to be approved for this offer.
- EPP Offer available for new activations and existing month to month users only. If an employee has a current TELUS Consumer agreement, they will have to be fully expired on their existing contract before they are eligible for the GoA EPP offer. Early contract buyouts are not permitted.
- The EPP offer is eligible to change. EPP users may be subject to rate plan changes with notice. These rate plan changes will take effect upon approval from the Government of Alberta Ministry of Service Alberta. All users on a month-to-month EPP agreement may be subject to these changes.

Users must purchase a new device from TELUS, aligned to the rate plan upon application for the TELUS GoA EPP Approved Affiliates offer.

Offer available with full-price, non-subsidized hardware only (hardware prices are subject to change). This excludes refurbished, unlocked and pre-paid devices. Limited to voice devices and smartphone devices only.

Available Hardware listings and pricing are available through your TELUS Authorized EPP Dealer or by visiting the TELUS Mobility website.

- TELUS may not offer some devices under the EPP program.
- TELUS Authorized EPP Dealers are eligible to charge an EPP activation fee. Please check with your TELUS Authorized EPP dealer to understand all costs associated with activating the GoA EPP offer.
- EPP offer for GoA Approved Affiliates employees is only available through certain authorized TELUS Dealers listed below.
- Offer can be fulfilled for any GoA Approved Affiliates employee across Alberta below by contacting one of the TELUS authorized Dealers.

Dealers listed will assist via email, phone or in-store sales. This Corporate offer is available Monday-Friday 8:00 AM-4:00 PM. Dealer store hours may vary.

TELUS Authorized GOA Approved Affiliates Dealers

These dealers can process any out-of-town orders:

Wireless City Edmonton
5912 104 Street
Edmonton, AB T6H 2K3
780 432 1100
mike@wirelesscityinc.com

Wireless City Calgary
264, 6100 Macleod Trail South
Calgary, AB T2H 0K5
403 517 1700
mike@wirelesscityinc.com



Clients activating on these plans can only select devices from the list of TELUS Devices associated with the Special Offer for Employees. Taxes, long distance, roaming and pay-per-use charges are extra. Additional fees may apply for servicing operations. Directory Assistance 411 Charge: \$2.50. Plus applicable provincial government 911 fees in Nova Scotia (43¢), P.E.I. (50¢), New Brunswick (53¢), Quebec (40¢) and Saskatchewan (52¢). Long distance refers to calls originating and terminating in Canada. Proof of employment is required. This pricing is only available while TELUS has a corporate agreement in effect with the company supporting the above offer and TELUS may terminate the availability of the Special Offer for Employees at any time. The "What You Get, What You Pay" brochure applies to TELUS consumer rate plans, and does not apply to the Special Offer for Employees set out above. Despite anything else in the TELUS Service Agreement or the Service Terms, if you are no longer employed by the company supporting the above offer, the Special Offer for Employees will no longer apply and TELUS will apply a rate plan generally available to TELUS consumer clients. TELUS considers 3 GB to be the average data use per month for a smart phone user. TELUS, the TELUS logo, and the future is friendly are trademarks of TELUS Corporation, used under license. All other trademarks are the property of their respective owners. © 2016 TELUS. 16_00175

