



MUNICIPAL DISTRICT OF GREENVIEW No. 16

POLICY REVIEW COMMITTEE

AGENDA

June 15, 2022

10:30 a.m.

Council Chambers/Zoom

#1 CALL TO ORDER

#2 ADOPTION OF THE AGENDA

#3 ADOPTION OF THE MINUTES

#4 POLICIES

| | |
|---|--------|
| 4.1 Policy 2004 Employee Code of Conduct | Pg. 6 |
| 4.2 Policy 2002 Disconnecting from Work | Pg. 15 |
| 4.3 Policy 1029 Records Management | Pg. 20 |
| 4.4 Policy 4006 Fleet and Equipment Replacement | Pg. 35 |
| 4.5 Town of Grande Cache Policy Repeal | Pg. 46 |

#5 NEXT MEETING DATE July 13, 2022

#6 ADJOURNMENT

Minutes of a
POLICY REVIEW COMMITTEE
MUNICIPAL DISTRICT OF GREENVIEW NO. 16
M.D. Administration Building, Council Chambers
Valleyview, Alberta, on May 11, 2022

1:
CALL TO ORDER

Chair Tom Burton called the meeting to order at 10:45 a.m.

PRESENT

| | |
|--|------------------------------------|
| Chair | Councillor Tom Burton |
| Member | Councillor Jennifer Scott |
| Member | Councillor Sally Rosson |
| Alternate Member | Councillor Dave Berry |
| Alternate Member | Deputy Reeve Bill Smith (virtual) |
| Alternate Member | Councillor Ryan Ratzlaff (virtual) |
| Alternate Member | Councillor Christine Schlieff |
| Alternate Member | Councillor Dale Smith |
| CAO | Stacey Wabick |
| Director of Infrastructure & Planning | Roger Autio |
| Director of Corporate Services | Ed Kaemingh |
| Director of Community Services | Michelle Honeyman |
| Manager of Agricultural Services | Sheila Kaus |
| Manager of Human Resources | Erin Klimp |
| Legislative Services Officer/Recording Secretary | Sarah Sebo |
| FOIP/Records Management Officer | Karen Chowace |
| Legislative Assistant | Drew Melvin |

ABSENT

| | |
|------------------|----------------------------|
| Alternate Member | Reeve Tyler Olsen |
| Alternate Member | Councillor Winston Delorme |

#2
POLICY REVIEW
COMMITTEE
AGENDA

MOTION: 22.05.115 Moved by: COUNCILLOR DUANE DIDOW.
That the Policy Review Committee adopt the Agenda of the Policy Review
Committee meeting as presented.

CARRIED

#3
POLICY REVIEW
COMMITTEE
MINUTES

MOTION: 22.05.116 Moved by: COUNCILLOR SALLY ROSSON.
That the Policy Review Committee adopt the minutes of the Policy Review
Committee meeting held on April 13, 2022, as amended.

- First three motions require CARRIED
- Dale Smith present

CARRIED

#4
BUSINESS

4.1 "Records Management"

Records Management

MOTION: 22.05.117 Moved by COUNCILLOR DALE SMITH:
That the Policy Review Committee recommend Council approve Policy 1029
"Records Management" as amended.

MOTION: 22.05.118 Moved by COUNCILLOR DAVE BERRY:
That the Policy Review Committee defer Policy 1029 "Record Management" to
the next Policy Review Committee.

CARRIED

Access to Information

4.2 "Access to Information"

MOTION: 22.05.119 Moved by COUNCILLOR JENNIFER SCOTT:
That the Policy Review Committee accept Policy 1042 "Access to Information"
as amended.

- Have FOIP listed in all instances where the record can be deferred to the FOIP coordinator
- Include Fire Department incident reports in Protective Services and Enforcement Services Reports

CARRIED

4.3 "Annual Ratepayers Barbecues"

Annual Ratepayers
Barbecues

MOTION: 22.05.120 Moved by: COUNCILLOR SALLY ROSSON.
That the Policy Review Committee recommend Council approve Policy 1039
"Annual Ratepayers Barbecues"" as amended.

- Include - Greenview partners will be invited to the BBQ to have a booth/presence at the discretion of administration.

CARRIED

MOTION: 22.05.121 Moved by: COUNCILLOR CHRISTINE SCHLIEF.

That the Policy Review Committee recommend Council repeal Policy CO-01
“Annual Ratepayers Barbecues”.

DEFEATED

4.4 “Payroll”

Payroll

MOTION: 22.05.122 Moved by: COUNCILLOR DUANE DIDOW.

That the Policy Review Committee recommend Council approve the transfer of Policy 2018 “Payroll” from a Council policy to an administrative policy as amended.

- Include definition for employee
- 3.6 All staff will be provided access to retrieve electronic advice slips

CARRIED

4.5 “Beaver Harvest Program”

Beaver Harvest Program

MOTION: 22.05.123 Moved by: COUNCILLOR DAVE BERRY

That the Policy Review Committee recommended Council approve Policy 6321
“Beaver Harvest Program” as amended.

- Purpose – related to problem beaver activity
- 1.1 “incentive program”
- 1.4 Problem Beaver means a beaver harvested in an area where operational and structural issues impacting municipal, private infrastructure and/or agricultural lands are being caused by beaver(s)
- 3.2 remove “prioritizing”
- 2.3 remove \$30.00 and have as per schedule of fees and require electronic payment
- Add a provision for potentially requiring random sight checks
- 2.1 a, b, c - at no cost to the landowner

CARRIED

4.6 "Town of Grande Cache Policy Repeal"

Town of Grande Cache
Policy Repeal

MOTION: 22.05.124 Moved by: COUNCILLOR DALE SMITH.

That the Policy Review Committee recommend Council repeal the following obsolete Town of Grande Cache policies:

- Business Incentives 305/15
- Citizen Engagement 438/12
- Code of Conduct for Members of Council and Council Committees 307/14
- Conflict of Interest 265/09
- Council Responsibilities 449/16
- Delegates Appearing Before Council 459/17
- Departure gift 265/09
- Donation and Sponsorship 204/14
- Honorarium and Compensation 554/17
- Joint Funding of Capital Projects with the Municipal District of Greenview No. 16 073/17
- Open Public Forum at Regular Council Meetings 340/14
- Orientation 265/09
- Property Tax Cancellation, Reduction and Refund 304/15
- Public Participation 250/18
- Risk Management 262/10
- Strategic and Long-Term Planning 439/12
- Street Naming and Renaming 353/15

CARRIED

#5
ADJOURNMENT

MOTION: 22.05.125 Moved by: COUNCILLOR SALLY ROSSON.

That this meeting adjourns at 12:31 p.m.

RECORDING SECRETARY

CHAIR



REQUEST FOR DECISION

| | | | |
|-----------------|---|--------------------------------------|---------------|
| SUBJECT: | Policy 2004 Employee Code of Conduct | | |
| SUBMISSION TO: | POLICY REVIEW COMMITTEE | REVIEWED AND APPROVED FOR SUBMISSION | |
| MEETING DATE: | June 15, 2022 | CAO: | MANAGER: |
| DEPARTMENT: | HUMAN RESOURCES | DIR: | PRESENTER: EK |
| STRATEGIC PLAN: | Governance | LEG: SS | |

RELEVANT LEGISLATION:

Provincial – N/A

Council Bylaw/Policy – N/A

RECOMMENDED ACTION:

MOTION: That Policy Review Committee recommend Council approve Policy 2004 “Employee Code of Conduct” as presented.

BACKGROUND/PROPOSAL:

On May 10, 2022 Council made the motion:

MOTION: 22.05.250 Moved by: COUNCILLOR TOM BURTON
That Council defer policy 2004 to Policy Review Committee.

Deputy Reeve Bill Smith, Councillor Dale Smith, Councillor Ratzlaff, Councillor Rosson, Councillor Berry, Councillor Burton, Councillor Scott, Councillor Schlieff, Councillor Didow

CARRIED

At Council, there was concern expressed regarding the implication of Policy 2004 on contractors who operate family businesses. To quell any misconceptions regarding what is a conflict of interest administration has updated the policy to reflect conflict of interest as actual, potential or perceived. Any personal relationship has the potential to have a conflict of interest, it is not dependent on family ties. Administration has also updated the definition of conflict of interest to reflect this.

As well, “or designate” has been added to all references to the Human Resources Manager through the policy. If they are away, they will appoint another member of their team to operate in relation to this policy.

BENEFITS OF THE RECOMMENDED ACTION:

1. The benefit of Council accepting the revised motion is that Greenview will have a robust policy which limits unacceptable employee behaviours.

DISADVANTAGES OF THE RECOMMENDED ACTION:

1. There are no perceived disadvantages to the recommended motion.

ALTERNATIVES CONSIDERED:

Alternative #1: PRC has the alternative to make additional amendments to the policy.

FINANCIAL IMPLICATION:

There are no financial implications to the recommended motion.

STAFFING IMPLICATION:

There are no staffing implications to the recommended motion.

PUBLIC ENGAGEMENT LEVEL:

Greenview has adopted the IAP2 Framework for public consultation.

INCREASING LEVEL OF PUBLIC IMPACT

Inform

PUBLIC PARTICIPATION GOAL

Inform - To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.

PROMISE TO THE PUBLIC

Inform - We will keep you informed.

FOLLOW UP ACTIONS:

Administration will bring the policy to Council for approval.

ATTACHMENT(S):

- Policy 2004 – Current
- Policy 2004 - Revised

Title: EMPLOYEE CODE OF CONDUCT

Policy No: 2004

Approval: Council

Effective Date: September 24,2013

Supersedes Policy No: (None)



MUNICIPAL DISTRICT OF GREENVIEW NO. 16

"A Great Place to Live, Work and Play"

Policy Statement: The Municipal District of Greenview No. 16 is an open, accessible, and accountable form of government. There is a shared responsibility for all employees to conduct themselves in an ethical and professional manner at all times.

Purpose: To clearly define and provide a universal understanding of the minimum level of accepted and expected ethical and professional behavior of all employees.

Principles:

1. Integrate the Code of Conduct into all elements of MD operations.
2. Meet or exceed all legal and ethical responsibilities.
3. Ensure fair, equitable, and consistent application of the Code of Conduct.
4. Protect the public interest.
5. Provide training in the Respectful Workplace program to all employees annually.

Approved: 13.09.584

CURRENT

Title: Employee Code of Conduct

Policy No: 2004

Effective Date:

Motion Number:

Supersedes Policy No: None

Review Date:



Purpose: To clearly define and provide a universal understanding of the minimum level of accepted and expected ethical and professional behavior all people who work for or represent the Municipal District of Greenview No. 16 (Greenview).

The policy is intended to provide a reference guide and does not address every conduct situation or circumstance that may arise.

1. DEFINITIONS

- 1.1. ~~Adult Interdependent Partner~~ means a person who has lived with a person in a relationship of interdependence:
 - i. ~~For a continuous period of not less than 3 years, or~~
 - ii. ~~Of some permanence, if there is a child of the relationship by birth or adoption,~~

Or the person has entered into an adult interdependent partner agreement with the other person in accordance with the Adult Interdependent Relationships Act, R.S.A. 2000, Chapter A-4.5.
- 1.2. **Conflict of Interest** means a situation in which a person is able to derive personal benefit from actions or decisions made in their official capacity. **when an employee has a private or personal interest that could influence or compete with, or be perceived to influence or compete with, the objectives of any Greenview operations or duties.**
- 1.3. **Greenview** means the Municipal District of Greenview No 16.
- 1.4. **Nepotism** means the practice among those with power or influence of favouring relatives or friends, especially by regarding matters of employment.
- 1.5. **Weapon** means any thing used, designed to be used, or intended for use in causing death or injury to any person, or for the purpose of threatening or intimidating any person.

2. POLICY STATEMENT

- 2.1. The Code of Conduct applies to all employees, contractors, and contract employees at Greenview.
- 2.2. Greenview will ensure fair, equitable, and consistent application of the Code of Conduct.
- 2.3. Unacceptable behavioral actions have been classified as either: hazardous to employee health and safety, criminal, a negative influence on workplace morale, or detrimental to the success of Greenview business.
- 2.4. Greenview will comply with all applicable laws and regulations, including local and provincial codes, rules and regulations, applicable treaties, and industry standards.

3. CONFLICT OF INTEREST

- 3.1. Employees are expected in all regards to conduct their duties with impartiality.
- 3.2. A conflict of interest may be actual, potential, or perceived.
 - i. Actual conflict: a situation in which an employee's personal or private interests improperly influence the performance of official duties and responsibilities or where a position is used for personal gain or in personal circumstances.
 - ii. Potential conflict: a situation where an actual conflict could reasonably exist in the future if mitigation strategies are not followed.
 - iii. Perceived conflict: a situation where no actual conflict exists, however, the situation could be perceived by a reasonable observer to be a conflict, whether or not it is the case.
- 3.3. Employees are in an actual conflict of interest and in violation of this Code of Conduct if they:
 - i. Take part in a decision while carrying out their duties, knowing that the decision might further a personal or private interest of the employee, their spouse, adult interdependent partner, child or any other personal relationship; or
 - ii. Use their public role to influence or seek to influence a government decision which could further a personal or private interest of the employee, their spouse, adult interdependent partner, child, or any other personal relationship; or
 - iii. Use or communicate information not available to the general public that was gained by the employee in the course of carrying out their duties, to further or seek to further a personal or private interest of the employee, their spouse, adult interdependent partner, child or any other personal relationship.
- 3.4. Where an actual or proposed business or financial interest of an employee, or of the employee's spouse, adult interdependent partner, child, or any other personal relationship is affected, appears to be affected or may be affected by actions taken or decisions made in which the employee participates in the course of their employment, the employee shall disclose the business or financial interest to the Manager of Human Resources, or designate.
- 3.5. Employees shall not accept fees, gifts or other benefits that are connected directly or indirectly with the performance of their public service duties, or for the purpose of

soliciting work, from any individual, organization, or corporation. Gifts may be exchanged internally amongst coworkers.

4. NEPOTISM

- 4.1. Employees who exercise regulatory, inspection or other discretionary authority over others shall disqualify themselves from dealing with anyone with whom the relationship between them may bring the employee's impartiality into question, with respect to those functions. In situations where this would impair service delivery, employees must advise the Manager of Human Resources, **or designate**, of the details before exercising their authority. Once the Manager of Human Resources, **or designate**, has been notified the employee shall only exercise their authority in accordance with instructions received. In emergency situations the employee shall act impartially and notify the Manager of Human Resources, **or designate**, immediately after exercising their authority.
- 4.2. Relatives of an employee may work in the same department provided there is no opportunity to exercise favouritism and no conflict of interest exists for the employees involved. An employee may not supervise a relative unless there are extenuating circumstances and the Manager of Human Resources, **or designate**, approves an exemption from this section of the policy.
- 4.3. In the staffing process, selection panel members shall disqualify themselves from competitions where applicants are relatives or other individuals, where the continued participation of the panel member could raise a question as to their impartiality.
- 4.4. Employees shall, so far as it is known to them, disclose and discuss with the Manager, **or designate**, of Human Resources situations which may be or may appear to be conflicts of interest under this section.

5. RELATING TO THE CAO

- 5.1. If a matter pertaining to the CAO arises, through CAO disclosure or otherwise, the Manager of Human Resources will provide a recommendation to the CAO regarding the appropriate action for the conflict of interest or nepotism in question. If the CAO disagrees with the Manager of Human Resources' decision, and the matter is unresolved, it will proceed to a review committee comprised of the four Directors, the Manager of Human Resources, **or designate, the Reeve, and the Deputy Reeve**. The review committee shall vote with the majority ruling. The decision of the review committee shall be final and binding and will be communicated to the CAO in writing.

6. CONSEQUENCES OF NON-COMPLIANCE

- 6.1. Greenview will address any infraction or instances of non-compliance and take correct action. All misconduct will be reviewed, as per the outlined procedures, and may result in disciplinary action, up to and including dismissal from employment, seeking restitution, commencement of civil action, criminal prosecution, or any combination thereof.

7. EXPECTATIONS

- 7.1. Commit to demonstrating Greenview values in their work and personal conduct.
- 7.2. Meet or exceed all legal and ethical responsibilities in their day-to-day work and personal conduct.
- 7.3. Employees are expected to perform their job duties in a manner conducive to a healthy and safe workplace, following all Greenview practices, policies, and procedures.
- 7.4. Abide by all Greenview policies in daily activities.
- 7.5. Act appropriately and reasonably when placed in compromising or situations where there is a real or perceived conflict of interest.
- 7.6. Employees are expected to operate Greenview equipment and vehicles in accordance with Greenview's Vehicle Usage Policy.
- 7.7. Recognize and maintain the highest level of confidentiality.
- 7.8. Be an ambassador – treat all citizens, vendors, and special interest groups fairly and consistently. Act and communicate in a way that reflects positively on Greenview.
- 7.9. Protect Greenview's reputation. As a Greenview employee, our behaviour is held to a higher standard when interacting with the media, making public statements, or using social media for work or personal use. You are accountable for your personal use of social media in the same way you are accountable for your off-duty conduct.
- 7.10. Work collaboratively to ensure quality service is provided to the ratepayers, Greenview communities, and surrounding areas.
- 7.11. Understand that this policy is further supported and complimented by other Greenview policies and standards including but not limited to Health and Safety, Workplace Violence and Respectful Workplace, Substance Abuse Prevention, and Social Media.
- 7.12. Understand that this policy is intended to support and complement any professional code of conduct or ethics that individuals are expected to follow due to their professional affiliation.

8. UNACCEPTABLE ACTIONS/BEHAVIOURS

- 8.1. Unacceptable behaviours shall include, but are not limited to the following:
 - A) Being under the influence of any non-prescribed drugs or alcohol while on Greenview premises, operating a Greenview vehicle, or are in the act of conducting Greenview business regardless of location.
 - B) Causing physical or emotional harm to another person;
 - C) Threats or harassing behaviour;
 - D) Aggressive behaviour that constitutes a reasonable fear of bodily harm to another person.

- E) Verbal assault, causing emotional duress.
- F) Willful damage or destruction to Greenview, or employee property;
- G) Possession of a weapon while on Greenview premises, while conducting business on behalf of Greenview. Exempted from this provision are employees who are required to use or discharge a weapon in the operation of their duties, or designated employees of Greenview, who may require the use of a firearm or weapon to destroy pests or immobilize animals.
- H) Disorderly, or indecent conduct on Greenview premises;
- I) Creating a disturbance that interferes with the normal job activities of other employees.
- J) Engaging in malicious gossip and/or the spreading of rumours;
- K) Causing an unsafe work environment, and thereby endangering the safety of Greenview employees;
- L) Violation of health and safety practices, policies and procedures;
- M) Theft, including physical and intellectual properties;
- N) Insubordination;
- O) Dishonest, illegal, or improper business activities;
- P) Job abandonment;
- Q) The use, possession, sale, manufacture or dispensation of any drug, alcohol, or paraphernalia associated with either;
- R) Failure to adhere to the requirements of any drug or alcohol treatment or counseling program in which the employee is enrolled;
- S) The use of alcohol or illicit narcotics off of Greenview premises that adversely affects the employee's work performance, the employee's own safety or the safety of others at work, or Greenview's reputation in the community;
- T) Failure to report to management the use of any prescribed drug which may alter the employee's ability to safely perform their duties;
- U) Repeatedly arriving to work late without providing advance notice and/or without reasonable cause;
- V) Failure to properly report an absence; and
- W) Failure to meet stated goals, objectives, and/or performance metrics required for a position.

By signing below, I acknowledge that I have read and understood this policy, and accept all responsibilities outlined within.

| | | |
|------------|-----------|------|
| | | |
| Print Name | Signature | Date |



REQUEST FOR DECISION

| | | |
|-----------------|--|---|
| SUBJECT: | Policy 2002 Disconnecting from Work | REVIEWED AND APPROVED FOR SUBMISSION |
| SUBMISSION TO: | POLICY REVIEW COMMITTEE | CAO: MANAGER: |
| MEETING DATE: | June 15, 2022 | DIR: PRESENTER: EK |
| DEPARTMENT: | HUMAN RESOURCES | LEG: SS |
| STRATEGIC PLAN: | Governance | |

RELEVANT LEGISLATION:

Provincial – N/A

Council Bylaw/Policy –

- Staff Agreement (2020)
-

RECOMMENDED ACTION:

MOTION: That the Policy Review Committee recommend Council approve Policy 2002 “Disconnecting from Work” as presented.

BACKGROUND/PROPOSAL:

Smartphones and e-communications are a reality of the workplace. Employees are increasingly subject to expectations to be constantly available. Greater access to workplace electronic communications is blurring the lines between on-duty and off-duty time. Employees should be able to disconnect from workplace communications channels outside normal working hours.

With the ability to always be connected, employees’ health may be at risk due to an imbalance between work and the need for rest (both physical and mental). Workers may also feel the need to stay connected out of fear of repercussions.

The right to disconnect was first introduced in France. The concerns that mobile technology could have a negative impact on work-life balance of French workers eventually led to the passing of a law to protect the rights of workers. Since then, four additional countries have adopted right-to-disconnect laws. In Canada, Ontario has adopted legislation requiring employers to create a “Disconnecting from Work Policy” by June 2, 2022.

It is not known at this time if Alberta will adopt similar legislation in the future however, as an employer, Greenview has a responsibility to protect the well-being of its employees.

Cognitive and emotional overload from hyper-connectivity can have negative effects including fatigue due to the psychosocial risk of being constantly connected. This can have both physical and mental health effects. The Disconnecting from Work Policy is a way to ensure a balance between work and private life.

BENEFITS OF THE RECOMMENDED ACTION:

1. Demonstrates that the health and wellbeing of Greenview employees is a priority.
 2. Provides clear expectations.
 3. Supports a commitment to overall employee health and wellness and provides employees with a positive work–life balance.
 4. Creates a workplace culture where employees feel they can disconnect from work and work-related devices during off-duty time.
-

DISADVANTAGES OF THE RECOMMENDED ACTION:

There are no perceived disadvantages to the recommended action.

ALTERNATIVES CONSIDERED:

Alternative #1: The Policy Review Committee has the alternative to alter or deny the recommended motion.

FINANCIAL IMPLICATION:

There are no financial implications to the recommended policy.

STAFFING IMPLICATION:

There are no staffing implications to the recommended motion.

PUBLIC ENGAGEMENT LEVEL:

Greenview has adopted the IAP2 Framework for public consultation

INCREASING LEVEL OF PUBLIC IMPACT

Inform

PUBLIC PARTICIPATION GOAL

Inform - To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.

PROMISE TO THE PUBLIC

Inform – We will keep you informed.

FOLLOW UP ACTIONS:

Administration will bring the policy to Council for approval.

ATTACHMENT(S):

- Policy 2002 Disconnecting from Work

Title: Disconnecting from Work

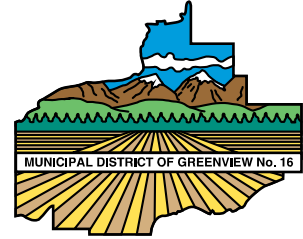
Policy No: 2002

Effective Date: Date passed in Council

Motion Number:

Supersedes Policy No: NONE

Review Date: (3 Years from date approved by Council)



Purpose: Prioritising the health and wellbeing of our employees is of the utmost importance to Greenview and we equally encourage and support our employees to prioritize their health and wellbeing while working and while away from work. To help employees achieve a healthy and sustainable work-life balance, Greenview recognises that every employee is entitled to switch off outside of their normal working hours, and enjoy their free time away from work without being disturbed unless there is an emergency, urgent matter, or agreement to do so. This policy also outlines Greenview’s commitment to employees, and the responsibilities of employees, to ensure there is a supportive work culture which enables employees to feel they can disconnect from work and work-related devices outside their normal working hours without repercussion.

1. DEFINITIONS

- 1.1. **CAO** means Chief Administrative Officer for the Municipal District of Greenview No. 16.
- 1.2. **Disconnecting from Work** means not engaging in work-related communications, including e-mails, telephone calls, video calls, text, or the sending or reviewing of other messages, to be free from the performance of work.
- 1.3. **Emergency** means an event that occurs and endangers Greenview elected officials, employees, clients, or the public; or has an imminent risk of disrupting workplace operations or causing catastrophic damage.
- 1.4. **Employee** means a person employed by Greenview, in any capacity.
- 1.5. **Greenview** means the Municipal District of Greenview No. 16.
- 1.6. **Normal working hours** means the time when employees are meant to complete work for Greenview excluding paid and unpaid breaks.
 - A) Full-time hours - 7.5 hours per day (37.5 hours in a work week).
 - B) Part-time hours - Up to 7.5 hours per day (less than 37.5 hours in a work week).
 - C) When required to be on-call or work overtime.
 - D) As specified in an Hours of Work Averaging Arrangement.
- 1.7. **Supervisor** means Council, CAO, Director, Manager or Supervisor or any other position title that determines an employee’s work schedule.

- 1.8. **Business Communications** means any type of communication, related to work, between individuals. This includes, but is not limited to:
 - A) Phone calls to desk phones, cell phones and home phones
 - B) Emails
 - C) Text Messages
 - D) Social Media messages
- 1.9. **Urgent Matter** means a situation that is not an emergency and cannot be addressed during normal working hours and that will have immediate consequences of a serious nature if not addressed outside of normal working hours.
- 1.10. **Work Week** means Sunday through Saturday

2. POLICY STATEMENT

- 2.1. Greenview is committed to maintaining high standards in the delivery of its services and to ensuring the safety, health, and wellbeing of its employees. Greenview respects the right of all employees to maintain a healthy work-life balance and to disconnect from work outside of their normal working hours to enjoy their free time without being disturbed. While technological advances have brought significant benefits to the workplace, this does not mean that employees are expected to be contactable and accessible outside of their normal working hours (apart from occasional legitimate situations when it is necessary to contact staff outside of normal working hours).
- 2.2. Greenview supports a culture where employees feel they can disconnect from work without repercussion.
- 2.3. Greenview understands that due to work-related pressures, the current landscape of work, or the working environment, employees may feel obligated to perform their job duties outside their normal working hours. Work-related pressure and feeling an inability to disconnect from the job can lead to stress and deterioration of mental and physical health.
- 2.4. Greenview will ensure a safe workplace in accordance with health and safety legislation, health and safety policies and best practice. Disconnecting from work is vital for employee wellbeing and to help achieve a healthy and sustainable work-life balance. Employees are encouraged and supported to prioritise their own wellbeing.
- 2.5. Some employees, depending on their role may be provided with handheld devices, including but not limited to a mobile phone, laptop or tablet. It is important to be aware that these are provided to allow flexibility and convenience in how employees complete their work. This does not imply that the employee must be connected to work at all times.

3. PROCEDURE

- 3.1. A joint approach from Greenview and its employees will be taken to recognise we all have an obligation to achieve disconnecting from work. Greenview grants its employees permission to disconnect from work.
- 3.2. All employees will be provided with written information, as part of their Terms of Conditions of Employment, regarding their normal working hours.

- 3.3. Supervisors will ensure that employees are aware of their work schedule, including on-call requirements and overtime arrangements.
- 3.4. All business communications should be done mindfully. It is unreasonable to expect instant responses for regular and day-to-day concerns, comments and questions. Communications outside of regular working hours are only appropriate in situations where Urgent Matters and Emergencies are present.
- 3.5. In the event of an urgent matter or an emergency, a phone call must be placed to applicable parties to ensure that no employee is expected to continuously monitor and respond to email or text messages.
- 3.6. While Management staff receive time in lieu of overtime, the expectation to receive and respond to business communications outside of normal work hours is still intended to be reasonable. A phone call is required, as stated in subsection 3.5, and electronic communication monitoring is therefore, not required outside of regular work hours.
- 3.7. Delayed delivery options should be used when knowingly sending electronic communications outside an employee's normal working hours and set to a specified delivery time on the next closest working day.
- 3.8. Employees on approved leave are not expected to respond to business communications. Every effort should be made to redirect inquiries, utilizing out of office and voicemails tools, to other employees who can be available, during regular work hours, for the duration of your absence.
- 3.9. Everyone has a duty to respect an employee's entitlement to disconnect outside of their normal working hours. Contacting employees outside their normal working hours should be the exception rather than the norm.
- 3.10. Greenview expects that all communications are in alignment with the intentions of this policy and that mindfulness and reasonableness are the guiding philosophies applied within this policy.

4. APPLICATION

- 4.1. This policy applies to all Greenview employees, and Council regarding the CAO.
- 4.2. This policy will not apply during declared States of Local Emergency.

5. COUNCIL RESPONSIBILITIES

- 5.1. Council will support the health and wellbeing of Greenview employees by supporting a work-life balance.
- 5.2. Council will support a workplace culture where Greenview employees feel they can disconnect from work without repercussion.
- 5.3. Council will also be encouraged to disconnect from work in conjunction with this policy.

6. ADMINISTRATION RESPONSIBILITIES

- 6.1. Administration will inform Greenview employees of this policy.
- 6.2. Administration will support the health and wellbeing of Greenview employees by supporting a work-life balance.
- 6.3. Administration will support a workplace culture where Greenview employees feel they can disconnect from work without repercussion.

DRAFT



REQUEST FOR DECISION

SUBJECT: Policy 1029 Records Management
SUBMISSION TO: POLICY REVIEW COMMITTEE
MEETING DATE: June 15, 2022
DEPARTMENT: CORPORATE SERVICES
STRATEGIC PLAN: Governance

REVIEWED AND APPROVED FOR SUBMISSION
CAO:
DIR:
LEG: SS

MANAGER:
PRESENTER: KC

RELEVANT LEGISLATION:

Provincial –

- Municipal Government Act;
- CAN/CGSB-72.34-2017 Electronic Records as Documentary Evidence; and,
- ISO 15489-1:2016 Information and documentation - Records management - Part 1: General

Council Bylaw/Policy – N/A

RECOMMENDED ACTION:

MOTION: That the Policy Review Committee recommend Council approve revised Policy 1029 “Records Management.”

BACKGROUND/PROPOSAL:

The revised Records Management policy provides a means of facilitating good record keeping practices and aims to foster accountability and transparency in records management, by explaining staff’s responsibilities in greater detail.

On May 11th the Policy Review Committee voted to defer Policy 1029 to the June meeting.

MOTION: 22.05.117 Moved by COUNCILLOR DALE SMITH:

That Policy Review Committee defer Policy 1029 “Record Management” to the next Policy Review Committee.

CARRIED

Since that time, the policy has been updated by administration to promote each department appointing a member of their team to be the overseer of proper record filing in that department. Policy 1029 now iterates that Greenview’s official record management system is the only acceptable location for employees to store records. As well, when a new software is introduced, everything in the obsolete system needs to be properly retained before it is decommissioned.

BENEFITS OF THE RECOMMENDED ACTION:

1. The benefits of Council accepting the recommended motion will ensure that Greenview's record keeping practices meet ARMA International's Generally Accepted Recordkeeping Principles of Accountability, Transparency, Integrity, Protection, Compliance, Availability, Retention and Disposition; and
2. Provide guidance to employees to consistently file the records they create, receive, or maintain into Greenview's central electronic records management system that will facilitate:
 - access to past documentation to make informed business decisions;
 - access the information necessary to respond quickly and effectively to customers;
 - proof of Greenview's actions and business decisions in the event of litigation, audit, or government investigation.

DISADVANTAGES OF THE RECOMMENDED ACTION:

1. There are no perceived disadvantages to the recommended motion.

ALTERNATIVES CONSIDERED:

Alternative #1: PRC may make additional recommendations.

FINANCIAL IMPLICATION:

There are no financial implications to the recommended motion.

STAFFING IMPLICATION:

This policy will increase staff involvement by placing the responsibility of consistently importing records they create, receive, or maintain into Greenview's ERMS to support the actions and decisions made in the conduct of their position and in support of business activities.

There is no staffing implication as it relates to staffing levels.

PUBLIC ENGAGEMENT LEVEL:

Greenview has adopted the IAP2 Framework for public consultation.

INCREASING LEVEL OF PUBLIC IMPACT

Inform

PUBLIC PARTICIPATION GOAL

Inform - To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.

PROMISE TO THE PUBLIC

Inform - We will keep you informed.

FOLLOW UP ACTIONS:

Administration will bring the policy to Council for approval.

ATTACHMENT(S):

- Policy 1029 Records and Information Management - Original
- Policy 1029 Records Management - Revised

Records and Information Management

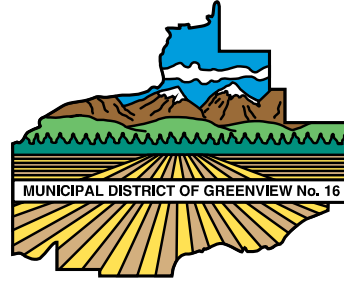
Policy No: 1029

Effective Date: Feb 25, 2019

Motion Number: 19.02.188

Supersedes Policy No: NA

Review Date:



Purpose: The purpose of the Records and Information Management (RIM) Policy is to set the direction for managing information regardless of the format of Greenview’s records; paper, digital and digital information systems.

Digital records are the official records of Greenview.

Greenview has adopted an approach to manage its records and information management program to ensure that records are created according to the business needs and business processes; adequately document the business activities in which they take part; are accurate and complete records of their activities; document policy formation and managerial decision making; provide transparency of record processes.

DEFINITIONS

Audit means the systematic review of recorded information activities for compliance with policies, procedures, and controls are established and complied with to meet all financial, operational, legal, and regulatory obligations.

Control means having the power or authority to manage, restrict, regulate, or administer the use or disclosure of a record. As per FOIP Act.

Business Records See Records

Destruction (Records) means the process of expunging records beyond any possibility of reconstruction and viewing.

Digital Information System means one or more computers; its software, peripherals, terminals, human operations, physical processes, and information transfer, that form an autonomous whole, capable of performing information processing and/or information transfer. Includes databases, ERP systems, GIS, etc.

Digital Record means a record that is carried by an electrical conductor and requires the use of electronic equipment to be understood.

Digitization means the process of rendering a paper record into an electronic image.

Documentary Evidence means recorded information admitted as evidence in legal proceedings

Electronic image means a source document that can be used to generate an intelligible reproduction of that document. In the case of paper source document, an intelligible reproduction means that:

- The reproduction is made with the intention of standing in place of the source document;
- The interpretation of the reproduction, for the purposes for which it is being used, gives the same information as the source document; and,
- The limitations of the reproduction (e.g., resolution, tone, or hues) are well defined and do not obscure significant details.

Electronic Records Management System (ERMS) means an information system primarily designed to assist in managing recorded information related to recordkeeping practices from inception to disposition of records.

Legal Hold means a process to preserve all forms of potentially relevant records when litigation is reasonably anticipated or underway.

Metadata means “data about data” structured information about a record’s characteristics (context, content, and structure) which helps to identify and manage that record.

Quality Assurance Program means a set of procedures based on the specifications of the ERMS which allows for monitoring and assessing its quality.

Records means information created, received, and maintained as evidence and as an asset, in pursuit of legal obligations or in the transaction of business.

Records Classification means the process of analyzing and determining the content and context of a record and selecting the function; the activity and transaction under which it will be filed and assigning the relevant metadata.

Source Document means an original from which a copy is made.

Transitory Records means copies or drafts of information retained elsewhere or records that will not be required as evidence of business activities. Have short-term value and which are:

- Not an integral part of functional classification system;
- Not required to sustain functional classification system;
- Not regularly filed under in the functional classification system;
- Not required to meet statutory obligations; and,

- Recorded only for the time required for completion of actions or ongoing records associated with them;
- Transitory records may be disposed of when they are no longer of value.

RESPONSIBILITIES

Records Management Coordinator Responsible for the Records and Information Management (RIM) Program records from their creation and preservation through to disposal.

Ensure that the RIM Program and the ERMS comply with the RIM policy, practices and procedures; the law, and national and industry standards so that the system will always produce and/or store records admissible as evidence.

Works with IT staff to integrate records management into Greenview’s usual and ordinary course of business, and to maintain that integration.

Maintain and amend the RIM Administration and Procedures manual with the support of IT staff so that it continuously reflects the exact state of the records system and can stand as evidence of the system’s compliance with the law and standards.

Identify the Records Management Coordinator responsibilities with respect to records quality assurance and for monitoring compliance with the support of IT staff.

Departments Support the implementation of the RIM Program across Greenview.

Users Ensure that all records are included in the ERMS.

REQUIREMENTS

The digital record is the official record of Greenview and are an integral part of its usual and ordinary course of business.

Records are managed in accordance with this policy, the RIM Administration and Procedures Manual and the Records Retention and Disposition Schedule Bylaw; and complies with applicable provincial and federal laws, national and industry standards.

Greenview has adopted the Generally Accepted Recordkeeping Principles to manage its information. In addition, this policy establishes the role of ERMS in the delivery business processes at Greenview.

Accountability

The RIM policy establishes the position of the Records Management Coordinator who with the support of IT staff is responsible for:

- The records and information management;
- Maintaining and amending the RIM policy, RIM Administration and Procedures manual and retention schedule;
- Integrating records and information management into the organization's usual and ordinary course of business;
- Quality assurance and for monitoring compliance and auditing for the creation, capture, management of authentic, reliable, and useable records that possess integrity, use, destruction, and preservation of records for as long as they are required;
- Maintaining the integration to continuously reflects the exact state of the digital records and digital information system so they can stand as evidence; and,
- Conduct periodic audits to verify compliance; and,
- Delivering record and information management training.

Transparency

The processes and activities of the RIM Program are documented in a manner that is open and verifiable and is available to personnel and appropriate parties.

- Transparency of information processes and the adequacy of records systems are maintained throughout the active life of the information;
 - Authentic;
 - Reliable;
 - Useable records; that,
 - Protect the integrity of those records for as long as they are required.
- Records and all information created or received by employees are the property of Greenview and should be managed as assets in compliance with all applicable laws, regulations, and standards.

Integrity

The RIM Program shall be constructed so the records and information generated or managed by or for Greenview have a reasonable and suitable guarantee of authenticity and reliability.

- Records are created, classified, scheduled, maintained, stored, and retrieved according to Greenview's policies and procedures and any applicable legislation.
- Employees create records, according to the business needs and processes that adequately document the business activities in which the employees are participants:
 - Supports the continuing conduct of business;
 - Complies with the regulatory environment;
 - Provides necessary accountability;

- Accurate and complete records of their activities;
- Document decisions, policy formation and business activities;
- Ensure transparency of record / business processes; and,
- Store all records in the ERMS system.

In addition, external service providers shall comply with this RIM policy and procedures and this provision shall be included in any contractual document or service standards and signs a confidentiality and privacy protection agreement or is otherwise contractually bound to protect Greenview from any breach of confidentiality or privacy.

Protection

The RIM Program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, or essential to business continuity.

- Policy dictates that an appropriate level of protection to records and information that are private, confidential, privileged, or essential to business continuity;
 - The chain of custody of the records is defined, when appropriate.
- Protect information against inappropriate or inadvertent information disclosure or loss incidents; and,
- Audit information is regularly examined, and continuous improvement is undertaken.

Compliance

The RIM Program shall be constructed to comply with applicable laws, regulations, and other binding authorities, as well as Greenview's policies and procedures.

The ERMS is created and maintained to comply with the procedures manual, provincial and federal laws, and national and industry standards.

Periodic audits shall be conducted to verify compliance.

Availability

Greenview shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Greenview backup systems are not considered records until they are used for recovery purposes.

Retention

Greenview shall maintain its records and information for an appropriate time, considering: administrative; legal and regulatory, fiscal, privacy, operational, and historical requirements.

The retention schedule shall be constructed in such a manner that:

- Facilitates the implementation of the retention and disposition schedule within the ERMS;
- Authorizes the disposition of source documents that have been imaged and captured in the ERMS system;
- All records and information assets destruction should be authorized by the Records Management Coordinator and business unit manager subject to the Records Retention and Disposition Schedule and the Records Legal Holds procedure.

In the event of the termination of business processes the records will be transferred to the Records Management Coordinator who will ensure their retention and disposition is in accordance with the records retention schedule.

Disposition

Greenview shall provide secure and appropriate disposition for records that are no longer required in accordance with the Records Retention and Disposition Schedule Bylaw.

- Records are maintained, stored, and preserved for the period of their usefulness to the organization and, if appropriate, to external stakeholders such as archival institutions and auditors;
- Electronic information is expunged, not just deleted, in accordance with retention policies.

DESIGN OF THE SYSTEM

Greenview has adopted a functional classification system which arranges records based upon the business functions performed by Greenview and its related work processes. This process is described in detail in the RIM Administration and Procedures Manual and also applies to digital information systems.

Use

The RIM Program has been adopted for use by all departments and agencies of Greenview.

Management

The RIM Program falls under the purview of Corporate Services.

Training

RIM Program and ERMS training will be provided by the Records Management Coordinator.

REVIEW

The RIM Policy and RIM Administration and Procedures Manual should be reviewed every three years.

Title: Records Management

Policy No: 1029

Effective Date: Date passed in Council

Motion Number:

Supersedes Policy No: 1029

Review Date: (3 Years from date approved by Council)



Purpose: The purpose of this policy is to establish a framework to manage records of all formats efficiently and effectively.

This policy establishes the Records Management Program to facilitate good record keeping practices that aims to foster accountability and transparency.

This policy will ensure that Greenview's official records are maintained, preserved, and disposed of in accordance with fiscal, operational, legal, and regulatory requirements.

This policy provides guidance to manage Greenview's records to ensure accordance with applicable legislation established by the Government of Alberta and Canada for the benefit of present and future generations.

1. DEFINITIONS

- 1.1 **Audit** means the systematic review of recorded information activities for compliance with policies, procedures, and controls are established to meet all financial, operational, legal, and regulatory obligations.
- 1.2 **Control** means having the power or authority to manage, restrict, regulate, or administer the use or disclosure of a record.
- 1.3 **Destroy** means the process of expunging records beyond any possibility of reconstruction and viewing.
- 1.4 **Digital Information System** means one or more computers; its software, peripherals, terminals, human operations, physical processes, and information transfer, that form an autonomous whole, capable of performing information processing and/or information transfer. Includes databases, ERP systems, GIS, etc.
- 1.5 **Digital Record** means a record that is carried by an electrical conductor and requires the use of electronic equipment to be understood.
- 1.6 **Digitize** means the process of rendering a paper record into an electronic image.
- 1.7 **Disposition** means the final retention action carried out on a record. This may include destruction, deletion, secure destruction or deletion, or transfer for archival review or to a third party.

- 1.8 **Electronic Image** means a source document that can be used to generate an intelligible reproduction of that document. In the case of paper source document, an intelligible reproduction means that:
- A) The reproduction is made with the intention of standing in place of the source document;
 - B) The interpretation of the reproduction, for the purposes for which it is being used, gives the same information as the source document; and,
 - C) The limitations of the reproduction (e.g., resolution, tone, or hues) are well defined and do not obscure significant details.
- 1.9 **Electronic Records Management System (ERMS)** means an information system designed to assist in managing recorded information related to recordkeeping practices from inception to disposition of records.
- 1.10 **Employees** means those employed and acting on behalf of Greenview, regardless of employment status: full-time, part-time, temporary, seasonal, agents and representatives.
- 1.11 **Exceptions** means records that must be retained in their original paper format:
- A) Contracts/agreements with wet signatures.
 - B) Land purchases, sales, leases, and transfers.
- 1.12 **Greenview** means the Municipal District of Greenview No. 16.
- 1.13 **Legal Hold** means a process to preserve all forms of potentially relevant records when litigation is reasonably anticipated or underway.
- 1.14 **Metadata** means “data about data;” structured information about a record’s characteristics (context, content, and structure) which helps to identify and manage that record.
- 1.15 **Quality Assurance** means a set of procedures based on the specifications of the ERMS which allows for monitoring and assessing its quality.
- 1.16 **Record** means information in any form includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers, and any other information that is digitally created, written, photographed, recorded, or stored in any manner, but does not include software or any mechanism that produces records.
- 1.17 **Records Classification** means the process of analyzing and determining the content and context of a record and selecting the function, activity and transaction under which it will be filed and assigning the relevant metadata.
- 1.18 **Source Document** means an original from which a digital record is made.
- 1.19 **Substantive Record** means a record that is created, received, distributed, controlled, or maintained by Greenview. The record provides documentary evidence of the activities, rights, obligations, and responsibilities and is judged to hold administrative, fiscal, legal, enduring, and personal information value.
- 1.20 **Transitory Record** means recorded information that has short-term, immediate or is judged to hold no administrative, fiscal, legal, enduring, and personal information value to the organization and will not be needed in the future.

- 1.21 **Vital Record** means records essential to resumption or continuation of operations after an emergency or disaster; records necessary to recreate Greenview's legal and financial position; and/or necessary to preserve the rights of Greenview, its employees, customers, and ratepayers.

2. POLICY STATEMENT

- 2.1 Greenview recognizes that records are valuable corporate assets, and that access, preservation and security must be ensured throughout a record's life cycle. Effective records management contributes to the overall operation and decision making of the municipality by maintaining records deemed to have fiscal, legal, regulatory, administrative, operational, evidentiary, or historical value.
- 2.2 This policy establishes the Records Management Program which sets direction to achieve efficient and effective records management practices that support service delivery and programs, fosters informed decision making, facilitates accountability, integrity, protection, compliance, availability, retention, disposition, and transparency.
- 2.3 This policy establishes the Records Management Manual which sets direction to employees for the capture, management, retrieval, storage, access, security, disposition, and destruction of records throughout a records lifecycle.
- 2.4 Greenview declares that records created, captured, received, controlled, or maintained are the property of Greenview and not the property of its employees.
- 2.5 Greenview declares that the ERMS, known as FileHold, is the official recordkeeping repository for all Greenview's substantive digital records.
- 2.6 Greenview declares that Greenview's substantive digital records shall be imported into Greenview's ERMS.
- 2.7 This policy declares that digital records entered in Greenview's ERMS are the official records of business.
- 2.8 This policy applies to all records, regardless of format, created, or received during business transactions in all aspects of organizational business and all business applications used to create and store records.
- 2.10 This policy applies to all Greenview employees who create, capture, receive, control, or maintain records for Greenview.
- 2.11 Greenview declares that substantive digital records shall not be filed in the following digital storage areas:
- A) Outlook or personal email accounts.
 - B) Personal, Network Drives and desktops.
 - C) SharePoint.
 - D) Greenview Webpage.
- 2.12 This policy applies to records that may be maintained in digital information systems which operate outside of the ERMS, yet also function as record keeping systems. They therefore require compliance with legislative obligations and standards of practice. Whenever

possible, these other digital information systems shall interface with the ERMS, or if appropriate, their records will be integrated into the ERMS.

~~2.13 The objective of this policy is to set direction to achieve efficient and effective records management practices that support service delivery and programs, fosters informed decision making, facilitates accountability, integrity, protection, compliance, availability, retention, disposition, and transparency.~~

3. PROCEDURE

3.1 Greenview has adopted the Generally Accepted Recordkeeping Principles to manage records that facilitates accountability, integrity, protection, compliance, availability, retention, disposition, and transparency.

3.2 Records shall be managed and comply in accordance with this policy and applicable provincial and federal laws, national and industry standards.

3.3 Records deemed an Exception shall be digitized and imported into the ERMS by the responsible department. The original paper record shall be promptly forwarded to the Records Management Coordinator.

3.4 Care and attention shall be paid to aging Greenview digital information systems and what will happen when a system is full or no longer useable. Should a database or other electronic records repository be the only source of specific records, then prior to decommissioning that system, all the relevant records within that system must be converted to more current technology to continue access and retention of those records.

3.3 Records deemed as Vital records shall be identified and preserved.

3.4 Records of historic value shall be preserved and may be forwarded to an approved archival agency.

3.5 In the event of litigation or an official Freedom of Information Protection Privacy (FOIP) request, a legal hold status shall be declared halting the destruction of records, organization wide.

4. COUNCIL RESPONSIBILITIES

4.1 Review and update this policy in accordance with the policy review schedule.

4.2 Support the Records Management Program.

5. ADMINISTRATION RESPONSIBILITIES

5.1 Chief Administrative Officer

- A) Recognize that records are valuable corporate assets.
- B) Provide leadership and support for the Records Management Program.
- C) Authorize the destruction of records in compliance with the Records Retention Bylaw.

5.2 Directors and Managers

- A) Recognize that records are valuable corporate assets.
- B) Support the implementation of the Records Management Program across Greenview.
- C) Are responsible for the records in the care of their department.

- D) **Appoint a representative, within their department, to sit on the Records Management Team.**
- E) Ensure departmental compliance with this policy.
- F) Ensure employees are aware of their obligations to manage information appropriately.
- G) Are responsible for approving departmental records destruction requests.
- H) Support the Records Management Coordinator to oversee the Records Management Program.
- I) Support the Records Management Coordinator in the designation and training of end-users.

5.3 Records Management Coordinator

- A) Administer the Records Management program.
- B) **Administer the Records Management Team.**
- C) Maintain and update the Records Management policy.
- D) Maintain and update the Records Management Manual.
- E) Ensure that the Records Management Program complies with the Records Management policy, practices and procedures, national and industry standards to ensure the program and ERMS always produces and/or stores records admissible as evidence.
- F) Ensure quality assurance, monitoring compliance and auditing for the creation, capture, management of authentic, reliable, and useable records which possess integrity, and the use, destruction, and preservation of records for as long as they are required.
- G) Determine what, if any, security classification or designation levels need to be attached to records.
- H) Ensure the timely destruction of records that are no longer required.
- I) Notify departmental managers of their duty to approve record destructions.
- J) Provide guidance in determining whether records and information or other material have an operational, fiscal, administrative, or informational/ historical value and must be protected from deterioration or loss.
- K) Provide a means of managing physical records.
- L) Arrange for the transfer of records designated as having historical value to the appropriate archival agency.
- M) Work with business units and departments to establish communication and training programs for records management.
- N) Create and conduct records management training.

5.4 Greenview Employees

- A) Comply with this policy and the records management manual.
- B) Create and maintain complete and accurate records which will serve as evidence of decisions, transactions, and business activities, while ensuring the quality, authenticity, and reliability of records.
- C) Work cooperatively and diligently to correct errors in records and reduce the risk of recurrence.
- D) Comply with the file classification system and retention periods.
- E) Ensure substantive records they create, receive, or control are accurately digitized and imported into the ERMS.
- F) Enter applicable metadata for each record imported into the ERMS.
- G) Follow naming conventions.
- H) Ensure records in their custody are protected from inadvertent release, damage, or destruction.
- I) Ensure records are not removed from Greenview premises unless such removal is required to conduct Greenview's business.

- J) Promptly return information to Greenview when the purpose for which the information was removed from Greenview premises has ended.
- K) Ensure that upon employment exit or transfer, all records in their custody are transferred to a supervisor or successor. This includes all physical, digital and email records.
- L) ~~Return all records to Greenview upon termination of employment or contractual relationship with Greenview.~~
- L) Ensure that transitory records in their care are destroyed when no longer required.

DRAFT



REQUEST FOR DECISION

| | | | |
|-----------------|---|--------------------------------------|---------------|
| SUBJECT: | Policy 4006 Fleet and Equipment Replacement Policy | | |
| SUBMISSION TO: | POLICY REVIEW COMMITTEE | REVIEWED AND APPROVED FOR SUBMISSION | |
| MEETING DATE: | June 15, 2022 | CAO: | MANAGER: |
| DEPARTMENT: | OPERATIONS | DIR: | PRESENTER: LB |
| STRATEGIC PLAN: | Governance | LEG: SS | |

RELEVANT LEGISLATION:

Provincial – N/A

Council Bylaw/Policy – N/A

RECOMMENDED ACTION:

MOTION: That Policy Review Committee approve Policy 4006 “Fleet and Equipment Replacement” as presented

BACKGROUND/PROPOSAL:

This policy is a complete update to follow the new 1507 Tangible Capital Assets Policy and 1034 Asset Management policy. There are corrections in the document on tracking maintenance and what is the future prospect of the document. The policy now also lists asset definitions. Tables have been updated and all changes are reflective of the recently approved policies.

The fleet and equipment replacements will be their own category as discussed in the 1507 tangible capital assets policy. Changes are to maximize vehicle and equipment life capabilities for Greenview business and to minimize the risk of injuries. In the last 10 to 15 years, progress has been made in upgrading functional capabilities and improving the safety features of Greenview fleet and equipment.

The policy will set the operational and capital budgeting requirements to maintain departmental fleet and equipment.

BENEFITS OF THE RECOMMENDED ACTION:

1. The benefit of the Policy Review Committee approving the recommended motion is that the policy will reflect the updated asset replacement standards in the Tangible Capital Asset policy.

DISADVANTAGES OF THE RECOMMENDED ACTION:

There are no perceived disadvantages to the recommended motion.

ALTERNATIVES CONSIDERED:

Alternative #1: The Policy Review Committee has the alternative to alter or deny the recommended motion.

FINANCIAL IMPLICATION:

There are no financial implications to the recommended motion.

STAFFING IMPLICATION:

There are no staffing implications to the recommended motion.

PUBLIC ENGAGEMENT LEVEL:

Greenview has adopted the IAP2 Framework for public consultation.

INCREASING LEVEL OF PUBLIC IMPACT

Inform

PUBLIC PARTICIPATION GOAL

Inform - To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.

PROMISE TO THE PUBLIC

Inform - We will keep you informed.

FOLLOW UP ACTIONS:

Administration will bring the policy to Council for approval.

ATTACHMENT(S):

- Policy 4006 Vehicle and Equipment Replacement – Current
- Policy 4006 Fleet and Equipment Replacement - Draft

Title: Vehicle and Equipment Replacement

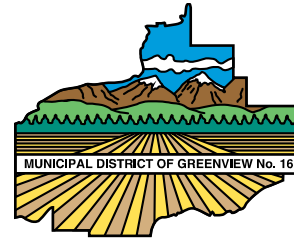
Policy No: 4006

Effective Date: May 11, 2020

Motion Number: 20.05.279

Supersedes Policy No: NONE

Review Date: May 11, 2023



Purpose: To ensure Greenview maintains a modern and reliable vehicle and equipment pool, at the lowest overall cost, through establishing a standard of equipment procurement, disposal, replacement and sustainable funding. Fire services equipment will be evaluated separately.

DEFINITIONS

ACAO means the Assistance Chief Administrative Officer.

CAO means Chief Administrative Officer.

CFO means the Chief Financial Officer.

GM means General Manager of one of the major departments and includes the Chief Financial Officer.

Greenview means the municipal corporation of the M.D. of Greenview No. 16.

Heavy Duty means a vehicle with a gross vehicle weight of greater than 10,000 lbs, including 1- ton trucks.

Life Cycle means the useful life of a vehicle or piece of equipment based on the average years, kilometres (km), or engine hours a vehicle or piece of equipment operates before maintenance becomes cost prohibitive.

Light/Medium Duty means vehicles with a gross vehicle weight of less than 8,500 lbs, including SUV’s, minivans, ½ ton trucks.

Medium Duty means vehicles with a gross vehicle weight of between 8,500 and 10,000 lbs, including ¾ ton trucks.

SLT means Senior Leadership Team comprised of the GMs, CFO, ACAO and CAO.

POLICY

General Principles

1. Administration will recommend the type of equipment and vehicles that will be required to be replaced on a regular basis, to ensure the services of Greenview are provided as directed by Council.
2. Administration will endeavor to purchase the most economical and fuel efficient vehicles and pieces of equipment available and will recommend for purchase the most basic vehicle to suit the department's needs
3. Used vehicles and pieces of equipment may be considered for purchase.
4. Administration may consider leasing vehicles or equipment when economically feasible.
5. All fleet acquisition and disposal will be conducted through the legislated procurement processes and in accordance with Greenview purchasing policies.
6. In circumstances where a vehicle or piece of equipment becomes cost prohibitive to maintain or operate, before the end of its established life cycle, it may be considered for early replacement.
7. Upon review, if a vehicle or piece of equipment has continually performed at a high level, with a satisfactory maintenance record, that vehicle or piece of equipment may be considered for a life cycle extension.
8. Vehicles and equipment will be evaluated for replacement based on the following criteria:

| VEHICLE/EQUIPMENT TYPE | TIME IN SERVICE (years/kms/engine hours/condition) |
|--|--|
| Light/Medium Duty Vehicles | 10 years / 200,000 kms |
| Medium Duty Diesel Vehicles | 10 years / 300,000 kms |
| Heavy Duty Vehicles | 10 years / 300,000 kms |
| Graders | 10 years / 7,500 hours |
| Loaders | 10 years / 7,500 hours |
| Backhoes | 10 years / 7,500 hours |
| Track Excavators | 7,500 hours |
| ATV's/UTV's | 15 years |
| Tractors (all types) | 7,500 hours |
| Zambonis | 10 years |
| Light Duty Mowers (zero -turn, self-propelled) | 5 years |
| Gang Mowers | 10 year |
| Water Tankers | 20 years |

Administrative Responsibilities:

9. Fleet Coordinator and Managers are responsible to recommend replacement of vehicles and equipment in accordance with this policy.
10. Vehicle accessories must be approved by the GM.

- 11. Vehicle replacement requests must be approved by the GM.
- 12. SLT must sign off on department requests for fleet vehicles above light/medium duty.

Equipment and Vehicle Fleet Reserve

- 13. Administration will establish an Equipment and Vehicle Fleet Reserve.
- 14. Administration will establish a Capital Reserve Replacement rate, taking into consideration the life span of the equipment and vehicle(s) and the estimated replacement cost.
- 15. Equipment and Vehicle Fleet Reserve replacement charges will be transferred to a capital reserve fund for equipment and vehicle replacement.
- 16. Fleet replacement and due to obsolescence or end of life cycle will be financed through the Equipment and Vehicle Fleet Reserve.
- 17. Fleet replacement due to physical damage will be financed through appropriate insurance procedures, with the balance for replacement coming from the vehicle replacement reserve.
- 18. Proceeds from the disposal of vehicles or equipment will be allocated to the Equipment and Vehicle Fleet Reserve.
- 19. Interest earned from the Equipment and Vehicle Fleet Reserve will be allocated to the reserve at year end.
- 20. Council shall authorize the transfer of funds to and from the reserve.

Title: Fleet and Equipment Replacement Policy

Policy No: 4006

Effective Date: Date passed in Council

Motion Number:

Supersedes Policy No: 4006

Review Date: (3 Years from date approved by Council)



Purpose: To ensure Greenview maintains a dependable, and reliable vehicle & equipment pool. The governance of **which is** fiscally responsible **and captures the** true value of assets through **the establishment of a** standard equipment procurement, disposal, and replacement policy. **Fire-Rescue Services Apparatus** and **Equipment** replacement will be evaluated separately.

1. DEFINITIONS

- 1.1. **Aircraft** means primarily for transportation purposes such as small airplanes, large planes, and other aircraft transporting devices. In this document is not to include emergency aircraft.
- 1.2. **Amortization** is the process of incrementally charging the cost of an asset to expense over its expected period of use, which shifts the asset from the balance sheet to the income statement. It essentially reflects the consumption of an intangible asset over its useful life. Amortization is most commonly used for the gradual write-down of the cost of those intangible assets that have a specific useful life.
- 1.3. **AMO** mean Asset Management Officer.
- 1.4. **Assets** are economic resources controlled by the municipality as a result of past transactions or events and from which future economic benefits are expected to be obtained. Assets have three essential characteristics:
 - A) They embody a future benefit that involves a capacity, singly or in combination with other assets, to provide future net cash flows, or to provide goods and services; and
 - B) The municipality can control access to the benefit, and;
 - C) The transaction or event giving rise to the municipality's control of the benefit has already occurred.
- 1.5. **Asset Disposal** refers to the removal of a tangible and / or non-tangible asset(s) from service as a result of sale, destruction, loss, or abandonment.
- 1.6. **CAO** means Chief Administrative Officer.
- 1.7. **Capital Lease** are non-financial assets leased by Greenview for use in the delivery of goods and services. All the benefits and risks of ownership are transferred to the municipality without requiring the transfer of legal ownership. This results in the recordation of the asset as Greenview's property in its general ledger as a fixed asset.

- 1.8. **Estimated Useful Life** is the estimate of the period over which a capital asset is expected to be used or the number of units of production that can be obtained from the asset. It is the period over which an asset will be amortized and is normally the shortest of the physical, technological, commercial, or legal life. This can be also to be referred to as useful life.
- 1.9. **Extended Warranty** also referred to as after sales service or simply service type warranty. Is an extra cost to the buyer on top of the purchase price. In such cases it is not capitalized and is deferred and reduced over the warranty term.
- 1.10. **Fleet** means all vehicle, operating equipment, and heavy equipment of Greenview.
- 1.11. **Fleet Management** refers to the overall actions that take place to keep a fleet running efficiently on time, and within budget
- 1.12. **Fleet and Equipment Replacement Reserve** This reserve ensures funds for replacing fleet and equipment as pertains to this policy.
- 1.13. **Greenview** means the Municipal District of Greenview No. 16.
- 1.14. **Heavy Mobile Equipment** means power and construction equipment such as graders, tractors, 3-point hitch mowers or bigger, mobile hot water/steam washers, gravel reclaimer, backhoe, ripper, mulcher, loaders, trencher, dozer, crawlers, agriculture equipment, all heavy equipment attachments, and Zambonis.
- 1.15. **Hours of Production Method** is an amortization method which allocated the cost of an asset based on its estimated hours of use or production.
- 1.16. **Life Cycle** means the useful life of a vehicle or piece of equipment based on the average years, kilometres (km), or engine hours a vehicle or piece of equipment operates before maintenance becomes cost prohibitive.
- 1.17. **Light Mobile Equipment** means equipment specific to maintenance, shop, and recreation mowers, lawn maintenance equipment, all-terrain vehicles (ATV), utility terrain vehicles (UTV), snowmobiles, drones, skid steers, and light mobile equipment.
- 1.18. **Operating Equipment** means equipment specific to maintenance, shop, recreation, and appliances such as forklifts, welding machines, utility trailers, security systems, snowplows, refrigerators, stoves, freezers, mowers, recreational equipment, generator, emergency operations equipment, and safety equipment.
- 1.19. **Repair and Maintenance** are ongoing activities to maintain a capital asset in operating condition. They are required to obtain the expected service potential of a capital asset over the estimated useful life. Costs for repairs and maintenance are expensed.
- 1.20. **SLT** means Senior Leadership Team comprised of Directors and the CAO.
- 1.21. **TCA** means Tangible Capital Assets.
- 1.22. **Vehicles** means primarily for transportation purposes such as automobiles, pick-up trucks under one ton, and sport utility vehicles (SUV). Vehicles in this policy do not include emergency vehicles.

1.23. **Vehicles Over 1 Ton** means equipment specific to maintenance and construction that can be used on municipal or provincial roads. These include but not limited to gravel trucks, various heavy equipment trailers, end dumps, pups, 3-ton trucks, 5-ton trucks, water trucks, garbage trucks, 1-ton trucks and vehicle maintenance trucks. For emergency Vehicles over 1 ton, please refer to policy 3021.

1.24. **Watercraft** means primarily for transportation purposes such as small boats, large boats, personal watercraft, remote control watercraft and other water transporting devices. Watercraft in this policy is not to include emergency watercraft, refer to Policy 3021.

2. POLICY STATEMENT

2.1. An effective fleet replacement program is essential for controlling fleet performance (i.e., vehicle and equipment suitability, availability, reliability, safety, and environmental impacts) and total cost of ownership.

2.2. Fleet management requires budgeting and a funding process that enables Managers, the AMO, the Procurement Officer and the Fleet Specialist to budget the amount of funds needed each year to execute the replacement plan based on the selected financing approach. The budgets for operation and maintenance comes from allocation of the overall operational budget and capital replacement is secured through the Fleet Replacement Equipment Reserve (Reserves Policy 1502).

2.3. Long-term fleet management replacement plans pinpoint anticipated replacement dates and costs of individual assets based on the application of recommended replacement cycles and quantifies year-to-year, fleet-wide replacement costs and future variations therein.

The Fleet Specialist, the AMO and Managers will recommend through a needs assessment, the type of equipment and vehicles that will be required to be replaced based on a schedule of useful life or hours of production. In addition, administration will provide council with a historical value and future demand for the vehicle or equipment being replaced. Maintaining Greenview's fleet and equipment ensures assets remain modern, dependable and reliable.

2.4. The Fleet Asset Management Plan (AMP) will have the information derived from the replacement plan, historical data, useful life per fleet asset and will include future demand on the fleet and equipment assets.

2.5. The Fleet Specialist with assistance from the Procurement Officer & the AMO will endeavor to purchase the most economical and fuel-efficient vehicles and pieces of equipment available. The Fleet Specialist and AMO will provide historical information, maintenance review and future demand of the asset, for the asset needs for the department.

2.6. A short-term replacement prioritization and earmarking process for designating specific vehicles and pieces of equipment to be replaced in the coming fiscal year. As per the table below.

2.7. Used vehicles and used pieces of equipment may be considered for purchase. These will be evaluated based on the historical information of the asset, maintenance, and current demand of the asset.

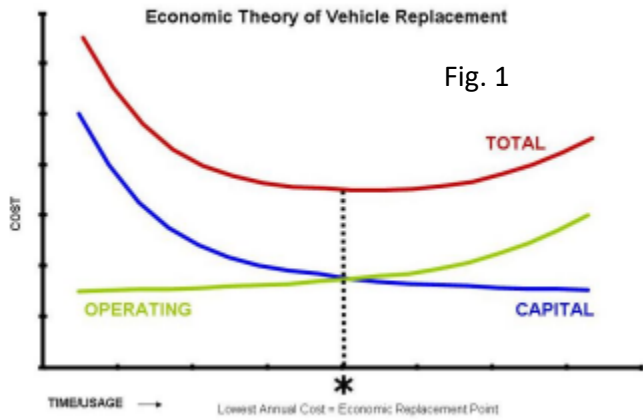
| VEHICLE/EQUIPMENT TYPE (According to the TCA Policy) | BASELINE TIME IN SERVICE (Years/kms/engine hours) |
|--|---|
| Vehicles | 5 years / 200,000 kms |
| Vehicle over 1 Ton | 10 years / 300,000 kms |
| Heavy Mobile Equipment | 20 years / 7,500 hours |
| Light Mobile Equipment * | 5 years |
| Operating Equipment | 10 years |
| Aircraft | 20 years |
| Watercraft | 20 years |

- 2.8. The Procurement Officer may consider capital leasing or rental of vehicles or equipment when economically feasible. If the arrangement is a capital lease or rental, Greenview should apply the thresholds of the appropriate capital or rental asset category.
- 2.9. All fleet acquisition and disposal will be conducted through the legislated procurement processes and in accordance with Greenview’s 1018 Procurement and Disposal Policy.
- 2.10. If a vehicle or piece of equipment has continually performed at a high level, with a satisfactory maintenance record, that vehicle or piece of equipment may be considered for a life cycle extension. This extension has no amortization to be assessed and could be looked at as a betterment of the asset. To be evaluated on a case-by-case basis.
- A) Extended warranty will apply to the asset for which it is purchased and will be deferred and recognized as an expense over the period offered as a straight-line basis.

3. PROCEDURE

- 3.1. Vehicles and equipment will be evaluated for replacement based on the following:
- A) TCA criteria, and;
 - B) The condition of vehicle performance based on Standards-Condition assessment of the Assets, and;
 - C) Maintenance records and costing.
- 3.2. Greenview will always consider longer service dates if equipment continues to perform well, meet minimum condition of fair standards, and are well maintained.
- A) Vehicle and equipment replacement guidelines should be based on the economic theory of optimal vehicle and equipment replacement, which is illustrated graphically in Fig. 1. As a vehicle and equipment age, its capital cost diminishes and its operating costs (e.g., maintenance, repair, and fuel) increase.

The combination of these two costs produces a U-shaped total cost curve that reflects the total cost of ownership of the asset. Ideally, a vehicle or piece of equipment should be replaced around the time the rise in annual operating costs begin to outweigh the decline in annual capital costs – that is, when the two cost curves intersect and the total cost of ownership begins to increase.



The total cost curve is different for every type of vehicle and, indeed, for every individual vehicle of a given type. This variability is caused by differences in the design and engineering of different types of vehicles / equipment, in operating environments, in the quality-of-care vehicles / equipment receives, and a variety of other factors.

- 3.3. Vehicle or equipment replacements are funded by the Fleet and Equipment Replacement Reserve.
- 3.4. First time purchases or additions to the current Greenview fleet and equipment pool cannot be financed with the Fleet and Equipment Replacement Reserve. Furthermore, all new vehicles and equipment must be approved by Council through a supplemental capital budget request.
- 3.5. Ensure all vehicles or equipment follow fleet management preventative maintenance program.
- 3.6. New type vehicle replacement requests must be approved by the Directors.
- 3.7. In circumstances where a vehicle or piece of equipment becomes cost prohibitive to maintain or operate, before the end of its established life cycle, it may be considered for early replacement / disposal.
- 3.8. Fleet replacement due to obsolescence or end of life cycle will be financed through the Fleet and Equipment Replacement Reserve. Noted as a capital replacement and approved by Council.
- 3.9. Fleet replacement due to physical damage will be financed through appropriate insurance procedures, with the balance for replacement coming from the Fleet & Equipment Replacement Reserve. The vehicle or equipment will be disposed of in accordance with 1018 Purchase & Disposal Policy.

4. COUNCIL RESPONSIBILITIES

- 4.1. Council is responsible for the capital budgets for the purchase of fleet / equipment assets
 - A) Each fleet / equipment asset must be listed for replacement as described in this policy.
 - B) Any unallocated capital Fleet / Equipment purchase funds will be transferred by Council back to the Fleet and Equipment Replacement Reserve.

5. ADMINISTRATION RESPONSIBILITIES

- 5.1. The Fleet Specialist, the AMO and Managers are responsible to recommend the replacement of vehicles and equipment through the needs assessment in accordance with this policy.
- 5.2. SLT must sign off on department requests for fleet vehicles / equipment for special cases or change in use.
- 5.3. Department lists must follow this policy
- 5.4. All safety equipment must be installed in the fleet asset before the asset is deemed ready for service.
- 5.5. All registration, licensing and insurance checks are needed per vehicle / equipment before the fleet asset is deemed ready for service.
- 5.6. All surplus / disposal listed fleet assets must have all safety equipment removed before being place on the surplus / disposal annual list.
- 5.7. All surplus / disposal listed fleet assets must have specialized / associated equipment removed before being place on the surplus / disposal annual list.
- 5.8. Surplus / disposal fleet asset lists are to be finalized annually in June of the year of the surplus / disposal.
- 5.9. Fleet and Equipment Replacement Reserve
 - A) Administration will follow a Fleet and Equipment Replacement Reserve. The reserve will operate in accordance Greenview's 1502 Reserve Policy.
- 5.10. Proceeds from the surplus / disposal of vehicles or equipment will be allocated to the Fleet and Equipment Replacement Reserve.



REQUEST FOR DECISION

| | | | |
|------------------------|---|---|----------------------|
| SUBJECT: | Town of Grande Cache Policy Repeal | | |
| SUBMISSION TO: | POLICY REVIEW COMMITTEE | REVIEWED AND APPROVED FOR SUBMISSION | |
| MEETING DATE: | June 15, 2022 | CAO: | MANAGER: |
| DEPARTMENT: | CORPORATE SERVICES | DIR: | PRESENTER: SS |
| STRATEGIC PLAN: | Governance | LEG: SS | |

RELEVANT LEGISLATION:

Provincial – N/A

Council Bylaw/Policy – N/A

RECOMMENDED ACTION:

MOTION: That the Policy Review Committee recommend Council repeal the following obsolete Town of Grande Cache policies:

- **Resolution No. 156/16 Acceptable Use of Communication/Technology Resources for Council**
- **Resolution No. 553/17 Council Electronic and Mobile Devices, Internet Access and Email Use**
- **Resolution No. 304/16 Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices (Procedure)**
- **Resolution No. 157/16 Guidelines for Acceptable Use of Communication Technology Resources (Procedure)**
- **Resolution No. 304/16 Information Access and Security – Physical, Electronic and Remote**
- **Resolution No. 304/16 Information and Records Management**
- **Resolution No. 304/16 Internet and Email Use**
- **Resolution No. 025/13 Municipal Emergency Management Policy**
- **Resolution No. 028/13 Municipal Notification of Emergencies Policy**
- **Resolution No. 304/16 Privacy Breach**
- **Resolution No. 304/16 Protection of Information and Privacy**
- **Resolution No. 304/16 Protection of Mobile Devices and Mobile Data Storage Devices**
- **Resolution No. 155/16 Records and Information Management and Security for Council**
- **Resolution No. 032/13 Training and Exercises Policy**
- **Resolution No. 399/18 Use of Surveillance Cameras**

BACKGROUND/PROPOSAL:

Administration reviewed the outstanding Town of Grande Cache policies and is recommending the following changes to harmonize administration between Ward 9 and the rest of Greenview.

- Acceptable Use of Communication/Technology Resources for Council 156/16 and procedure 156/16 Guidelines for Acceptable Use of Communication Technology Resources shall be repealed and replaced with Policy 1031 Cyber Security and Policy 1019 Issuance of Digital Communications Tools. Policy 1019 establishes the procedures for the issuance and maintenance of communication tools, and Policy 1031 outlines rule for communication tool holders.
- Acceptable Use of Communication/Technology Resources for Council 156/16 shall be repealed and replaced with Policy 1031 Cyber Security and Policy 1019 Issuance of Digital Communications Tools. Policy 1019 establishes the procedures for the issuance and maintenance of communication tools, and Policy 1031 outlines rule for communication tool holders.
- Council Electronic and Mobile Devices, Internet Access and Email Use 553/17 16 shall be repealed and replaced with Policy 1031 Cyber Security and Policy 1019 Issuance of Digital Communications Tools. Policy 1019 establishes the procedures for the issuance and maintenance of communication tools, and Policy 1031 outlines the rules for communication tool holders.
- Information Access and Security – Physical, Electronic and Remote 304/16 and procedure 304/16 Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices (Procedure) shall be repealed and replaced with Policy 1031 Cyber Security and Policy 1019 Issuance of Digital Communications Tools. Policy 1019 establishes the procedures for the issuance and maintenance of communication tools, and Policy 1031 outlines rules for communication tool holders.
- Information and Records Management 304/16 shall be repealed and replaced with Policy 1029 Records and Information Management and Bylaw 19-817 Records Retention and Disposition Schedule. Policy 1029 details the individual and institutional procedures to ensure the proper storage of data and records. Bylaw 19-817 legislates how long records must be kept and the manner in which they may be destroyed.
- Internet and Email Use 304/16 shall be repealed and replaced with Policy 1019 Issuance of Digital Communications Tools and Policy 1031 Cyber Security. Policy 1019 establishes the procedures for the issuance and maintenance of communication tools, and Policy 1031 outlines the rules for communication tool holders.
- Municipal Emergency Management Policy 025/13 shall be repealed and replaced with Bylaw 20-851 Municipal Emergency Management Bylaw. Bylaw 20-851 establishes the chain of command in the event of an emergency, it also creates the organisation and standards as they pertain to municipal emergency management.
- Municipal Notification of Emergency 028/13 shall be repealed and replaced with Bylaw 20-851 Municipal Emergency Management Bylaw. Bylaw 20-851 gives the responsible parties the

responsibility of notifying provincial and municipal authorities, as well as the public of an emergency.

- Privacy Breach 304/16 shall be repealed and replaced with Policy 1031 Cyber Security. Policy 1031 sets the standards to ensure the security of Greenview technology, and also creates the reporting procedure for any cyber security breaches.
- Protection of Information and Privacy 304/16 shall be repealed and replaced with Policy 1029 Records Information Management and Policy 1042 Access to Information. Policy 1029 establishes how and where municipal records are to be stored, whereas Policy 1042 establishes the procedures of record release.
- Protection of Mobile Devices and Mobile Data Storage Devices 155/16 shall be repealed and replaced with Policy 1019 Issuance of Digital Communications. Policy 1019 details the protocol when there is a real or perceived cyber security breach.
- Records and Information Management and Security for Council 155/16 shall be repealed and replaced with Policy 1029 Records and Information Management and Bylaw 19-817 Records Retention and Disposition Schedule. Policy 1029 establishes the procedure to archive records, as well as the location and length with which records must be kept. Bylaw 19-817 legislates how long records must be kept and the manner in which they may be destroyed.
- Training and Exercises Policy 032/13 shall be repealed and replaced with Bylaw 20-851 Municipal Emergency Management Bylaw. Bylaw 20-851 establishes the parties responsible to receive emergency management training as prescribed by the Alberta Emergency Management Agency.
- Use of Surveillance Cameras 399/18 shall be repealed and replaced with Policy 4005 Use of Surveillance Cameras. Policy 4005 details Greenview’s position on the use of surveillance equipment and the procedure for the implementation of such equipment.

BENEFITS OF THE RECOMMENDED ACTION:

The benefit of the Policy Review Committee recommending the repeal is to harmonize the administration of Ward 9 with the rest of Greenview.

DISADVANTAGES OF THE RECOMMENDED ACTION:

There are no perceived disadvantages to the recommended motion.

ALTERNATIVES CONSIDERED:

Alternative #1: The Policy Review Committee has the alternative to alter or deny the recommended motion.

FINANCIAL IMPLICATION:

There are no financial implications to the recommended motion.

STAFFING IMPLICATION:

There are no staffing implications to the recommended motion.

PUBLIC ENGAGEMENT LEVEL:

Greenview has adopted the IAP2 Framework for public consultation.

INCREASING LEVEL OF PUBLIC IMPACT

Inform

PUBLIC PARTICIPATION GOAL

Inform - To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.

PROMISE TO THE PUBLIC

Inform - We will keep you informed.

FOLLOW UP ACTIONS:

Administration will follow up on the recommendations of the Policy Review Committee, and afterward to Council.

ATTACHMENT(S):

- Resolution No. 156/16 Acceptable Use of Communication/Technology Resources for Council
- Resolution No. 553/17 Council Electronic and Mobile Devices, Internet Access and Email Use
- Resolution No. 304/16 Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices (Procedure)
- Resolution No. 157/16 Guidelines for Acceptable Use of Communication Technology Resources (Procedure)
- Resolution No. 304/16 Information Access and Security – Physical, Electronic and Remote
- Resolution No. 304/16 Information and Records Management
- Resolution No. 304/16 Internet and Email Use
- Resolution No. 025/13 Municipal Emergency Management Policy
- Resolution No. 028/13 Municipal Notification of Emergencies Policy
- Resolution No. 304/16 Privacy Breach
- Resolution No. 304/16 Protection of Information and Privacy

- Resolution No. 304/16 Protection of Mobile Devices and Mobile Data Storage Devices
- Resolution No. 155/16 Records and Information Management and Security for Council
- Resolution No. 032/13 Training and Exercises Policy
- Resolution No. 399/18 Use of Surveillance Cameras



TOWN OF GRANDE CACHE
Policy and Procedures

Title **Acceptable Use of Communication and Information Technology Resources** Page 1 of 7

Section FOIP/IT Security
Department All

Resolution No. 304/16
Effective Date June 8, 2016

P
O
L
I
C
Y

Background

The Town of Grande Cache (the ‘Town’) is committed to safe and responsible use of communication and information technology resources to protect the Town’s reputation and ensure responsible use of taxpayer dollars. This policy protects the interests of both the Town and the users of the Town’s communication and technology resources by providing a standard by which questions of acceptable communication and information technology resources use may be gauged.

1.0 Purpose

The purpose of this policy is to describe what the Town expects regarding acceptable uses of Town’s communication and information technology resources.

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Communication and Information Technology (IT) Resources that is any means by which information is exchanged between individuals through a common system, which includes, but is not limited to:

- a) computers (desktop, portable and wireless computing devices) and monitors;
- b) mobile computing devices including but not limited to notebook computers, laptops, tablets, cell phones, smart phones (ie. Blackberry, iPhone), air cards, push to talk radios and modems;
- c) internet and electronic communication services (email, instant messenger, voice mail, long distance and roaming, voice/text/data transmission, etc.);
- d) network infrastructures (ie. fiber optics cables, wireless networks, wi-fi access, etc.);
- e) photocopiers, fax machines, printers, scanners, cameras, radios, televisions, audio/visual equipment and desktop telephones;



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Acceptable Use of Communication and Information Technology Resources | Page 2 of 7 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

- f) business systems, office productivity systems, utility and all other Town-administered systems and related server and storage infrastructure;
- g) consumable goods used in the operation of these resources including but not limited to DVD's, CD's, tape media, paper, USB memory sticks, etc.; and
- h) all data, information online services and software applications which can be accessed using the above mentioned, including electronic mail, internet and chat technologies.

Communication and Information Technology Resource Users includes but are not limited to Town of Grande Cache employees, vendors, contractors, consultants and any other individuals with authorized access to and use of the Town communication and technology resources.

Contractor is any affiliate, third party, non-employee, consultant or agent or employee of a contractor or service provider engaged by the Town to perform services for or on behalf of the Town.

Data is a general term used to denote any or all facts, numbers, letters and symbols that refer to or describe an object, idea, condition, situation or other factors in a computerized form.

Department is an internal administrative division of the Town including all Town offices.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

FOIP Act means the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 as amended.

Information means any information that identifies an individual or business and is stored in any format that the Town utilizes in the usual business operations of the municipality.

IT Resource means any Town-owned or controlled asset used to generate, process, transmit, store or access Town information.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Acceptable Use of Communication and Information Technology Resources | Page 3 of 7 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

IT Resource Officer means the individual designated by the Chief Administrative Officer and has the responsibility to manage and control communication and technology resources for the Town.

User means any person authorized to access and/or use Town IT resources.

3.0 **Policy**

3.1 **Scope**

This policy applies to all Town employees and contractors (hereinafter referred to as ‘Users’) whose access to or use of information, communication and information technology (‘IT’) resources that is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town’s premises or elsewhere.

3.2 **Ownership**

3.2.1 All communication and IT resources acquired and managed by the Town, the data, information and the work product (ie. software programs, databases, spreadsheets, etc.) created, received or downloaded from external sources and/or modified in the use of such resources, belong to the Town of Grande Cache or its licensors.

3.2.2 All information created with or stored on Town communication and IT resources is the property of the Town.

NOTE: Employees should be aware and not expect that their communications are private when using Town communication and IT resources. Any information created with or stored on Town communication and IT resources may be considered a public record subject to disclosure under the FOIP Act.

3.3 **General Principles for Use**

3.3.1 The Town’s communication and IT resources are provided to improve productivity of Town business activities and enhance the effectiveness of communications.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Acceptable Use of Communication and Information Technology Resources | Page 4 of 7 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

3.3.2 The Town’s communication and IT resources must be used only for their intended purpose, as described in the ‘Guidelines for Acceptable Use of Communications and Technology Resources’ related to this policy.

3.3.3 Users of the Town’s communication and IT resources are required to use communication and IT resources in an acceptable manner as defined in the following:

- a) Information Access and Security Policy;
- b) Internet and Email Policy;
- c) Protection of Mobile Devices and Mobile Data Storage Devices Policy and Guidelines;
- d) Protection of Information and Privacy Policy;
- e) Employee Code of Conduct Policy; and
- f) Guidelines for Acceptable Use of Communication and Information Technology Resources.

3.4 Consent

3.4.1 Users of Town communication and IT resources are deemed to have given consent to this policy by their continued use of Town communication and IT resources.

3.5 Use of the Town’s Communication and Information Technology (IT) Resources for Electronic Communications and Internet Access

3.5.1 Use of Town communication and IT resources must be legal, ethical and in compliance with the Information Access and Security, Internet and Email Use and Employee Code of Conduct policies.

3.5.2 No user of the Town’s communication and IT resources should expect privacy as to his or her internet use.

3.5.3 Access to the electronic communications system and the internet is provided to the users of the Town’s communication and IT resources to enable them to carry out their job responsibilities.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|---|-----------------------|--------------|
| Title | Acceptable Use of Communication and Information Technology Resources | | Page 5 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

3.5.8 The Town does not manage, support or reimburse for personally owned communication and IT resources (ie. personal handheld wireless devices and airtime, ISP connections, home computers or software for personal use, etc.).

3.6 Safeguarding Assets, Data and Information

3.6.1 The Town’s communication and IT resources are valuable assets. Communication and IT resource users are expected to exercise reasonable care to prevent abuse or theft of the Town’s communication and IT resources.

3.6.2 The Town’s communication and IT resources are to be used in a manner that safeguards the integrity and accessibility of data, information and the work product (ie. software programs, databases, spreadsheets, etc.) created, received or downloaded from external sources and/or modified in the use of such resources.

3.6.3 All data or information which users consider sensitive or vulnerable must be encrypted with a Town-approved encryption solution, as outlined in the ‘Information Access and Security’ and ‘Internet and Email Use’ policies.

3.6.4 All PC’s, laptops and workstations are to be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device is left unattended. Because information contained on mobile devices is especially vulnerable, users must follow the ‘Protection of Mobile Devices and Mobile Data Storage Devices’ policy and guidelines to protect access to the device.

3.7 Responsibilities Related to the Town’s Communication and Information Technology Resources

3.7.1 Managers and supervisors are responsible for:

- a) ensuring employees are knowledgeable of the contents of this policy;
- b) reviewing and approving department communication and IT resources;
- c) providing users of the Town’s communication and IT resources with access to necessary training to use communication and IT resources efficiently and effectively;



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Acceptable Use of Communication and Information Technology Resources | Page 6 of 7 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

- d) informing the Chief Administrative Officer or designate of any breach of this policy;
- e) approving employee access to the Town’s communication and IT resources while on vacation or away on Town business (remote access);
- f) taking appropriate action, as defined in this policy, with respect to any breach of this policy.

3.7.2 Users of the Town’s communication and IT resources are responsible for:

- a) adhering to this policy;
- b) becoming as proficient in the use of communication and IT resources that are provided, as is necessary to fulfill work responsibilities;
- c) promptly advising managers or supervisors if any inappropriate or improper message or material is received; and
- d) immediately reporting any loss or theft of the Town’s communication and IT resources to the Chief Administrative Officer or designate.

3.8 Complying with Existing Laws and Town Policies

3.8.1 The Town’s communication and IT resources must be used in activities in compliance with all applicable laws or regulations, including without limitation, those:

- a) at the federal, provincial and municipal level;
- b) those by way of international treaties;
- c) those of any foreign jurisdiction with authority;
- d) those civil laws in force between vendor and purchaser of communication and IT resources; and
- e) any and all Town policies.

3.8.2 The Town’s communication and IT resources are to be used in a manner consistent with the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 and related Town policies.

The Town of Grande Cache has ZERO TOLERANCE for the use of Town assets in a way that could be deemed as offensive or harassing, such as hate mail, racial or ethnic slurs, insults, obscenities, abuse, defamation, threats, sexually explicit materials and internet gambling.

Accessing, communicating, creating distributing, viewing, sending, displaying or downloading of these inappropriate materials will be severely dealt with.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Acceptable Use of Communication and Information Technology Resources | Page 7 of 7 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

3.9 Consequences of Non-Compliance

- 3.9.1 Any use of Town communication and IT resources that breaches this policy will be considered misconduct and will be reviewed.
- 3.9.2 Any violation of this policy may subject the employee to their loss of use of communication and IT resources, and may result in disciplinary actions being taken, up to and including dismissal from employment.
- 3.9.3 Illegal acts involving communication and IT resources may also subject the user to restitution, commencement of civil action, or criminal investigation and prosecution by police agencies and/or local, provincial and federal authorities.

3.10 Unacceptable Use of the Town's Communication and Information Technology Resources

- 3.10.1 Unacceptable use of the Town's communication and IT resources includes, but is not limited to, knowingly or intentionally doing or allowing any of the following:
 - a) intercepting or altering data transmitted via technology resources;
 - b) violating terms of applicable software licensing agreement, including installing software without a license to do so;
 - c) using the Town's network to gain unauthorized access to any computer system or data;
 - d) moving computer equipment (except for portable devices), including all hardware and software components;
 - e) connecting unauthorized equipment to the Town's network;
 - f) attempting to circumvent the Town's communication and IT resources protection schemes;
 - g) activities that interfere with the normal operation of the Town's communication and IT resources;
 - h) using the Town's communication and IT resources for personal use that results in the Town incurring costs (ie. purchase and download of games, ringtones, wireless TV, video and music downloads, premium messaging subscriptions, storing of personal data on the Town's communication and IT resources, etc.); and
 - i) unauthorized use, or infringement, or theft of data, equipment, or tangible or intangible property, or any intellectual property rights thereto.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|---|-----------------------|------------------|
| Title | Council Electronic and Mobile Devices, Internet Access and Email Use | | Page 1 of 3 |
| Section | FOIP/IT Security | Resolution No. | 553/17 |
| Department | Council | Effective Date | November 8, 2017 |

P

1.0 Purpose

The purpose of this policy is to establish guidelines for the provision and use of electronic and mobile devices, wireless internet access at the Town/Council Offices and Council Chambers and email resources for Council members.

O

This policy replaces the 'Council Communication Device' policy, approved September 18, 2013 by Resolution No. 250/13.

2.0 Policy Statement

L

The Town of Grande Cache recognizes the importance of its Council members, in the performance of their duties, to be able to access information and communicate with each other, Town staff and other stakeholders in a timely and efficient manner. In support of this, the Town shall provide each Council member with an electronic device which may be a tablet, iPad or laptop computer and email resources during their term of office. The Mayor may be provided with a mobile device which may be a cellular phone or smartphone.

I

3.0 Policy Guidelines and Principals

C

- 3.1 Upon being elected, all Council members shall be provided with:
- a) a new electronic device, being a tablet, iPad or laptop computer;
 - b) an email address (____.____@grandecache.ca) for which all Town/Council business shall be conducted and channeled through the Town email server; and
 - c) wireless internet access at the Town and Council Offices and Council Chambers.

Y

- 3.2 The Mayor shall be issued a mobile device, which may be a cellular phone or smartphone, pursuant to this policy and will adhere to the principals and policies associated with this policy.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|--|
| Title | Council Electronic and Mobile Devices, Internet Access and Email Use | Page 2 of 3 |
| Section | FOIP/IT Security | Resolution No. 553/17 |
| Department | Council | Effective Date November 8, 2017 |

- 3.3 All electronic and mobile devices issued to Council members are the property of the Town of Grande Cache.
- 3.4 Council members are responsible for securing the information and protecting the integrity of the information on the Town-issued device in their possession, as set out in the 'Council Records and Information Management Policy'.
- 3.5 Each Council member shall receive a monthly allowance to assist with costs associated for electronic devices (ie. cell phone, home or laptop computer) and/or internet/wi-fi services, as set out in the 'Council Honorarium and Compensation Policy'.
- 3.6 Council members have the option to purchase the computer/tablet and/or cell phone at the end of their active service at a depreciated value as outlined below:
 - a) the device lifespan is approximately 3 to 4 years, at the end of which, Council members will be allowed to keep the device issued to them at no charge;
 - b) following an election, if a Council member leaves office prior to the end of the term, they will be allowed to purchase the device through a pro-rated amount of 50% after one year, 25% after two years and no charge after three years.
- 3.7 Town staff shall be responsible for:
 - a) selecting the electronic device and associated software;
 - b) setting up the electronic device and email service;
 - c) providing technical support for issues with the electronic device, installed software, email service; and
 - d) wireless internet access at the Town and Council Offices and Council Chambers that are directly related to Town business.
- 3.8 Council members shall make the electronic device available to Town staff for regular maintenance, software installation and updates, etc. upon request.
- 3.9 The loss or damage of an electronic device shall be reported immediately to the Chief Administrative Officer or designate. If the device is broken or not working properly, it must be returned to the Town Office for repair and/or replacement.
- 3.10 Council members may use the electronic device for personal use provided that such use does not result in increased costs to the Town and complies with this policy.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|--|
| Title | Council Electronic and Mobile Devices, Internet Access and Email Use | Page 3 of 3 |
| Section | FOIP/IT Security | Resolution No. 553/17 |
| Department | Council | Effective Date November 8, 2017 |

- 3.11 The Town of Grande Cache is not responsible for the loss or corruption of personal information contained on the Council member’s electronic device.
- 3.12 Acceptable electronic device, Town wireless internet access and email uses and activities by Council members are those that conform to the Town’s vision, mission and key principles and shall:
- a) respect and uphold the law, including provincial and federal laws and regulations and the law of other jurisdictions;
 - b) comply with the Town’s stated policies, procedures and standards;
 - c) be used responsibly and for the uses for which they were intended;
 - d) be courteous and follow accepted standards of etiquette; and
 - e) protect others’ privacy and confidentiality.
- 3.13 The Town of Grande Cache shall not be held liable for Council member’s unauthorized, inappropriate or illegal use of the Town’s electronic device, installed software, wireless internet access at the Town and Council Offices and Council Chambers and email resources.
- 3.14 Upon expiry of their term of office, Council members shall return the electronic device to the Town if they do not wish to keep it, as outlined in section 3.6 above. The Town will discontinue the Council member’s email address and the Council member’s use of the Town’s wireless internet and email resources will cease.

References

Council Honorarium and Compensation Policy, Section C-1: Council, Town of Grande Cache Policy and Procedures Manual

Council Records and Information Management, Section F-1: FOIP and IT Security, Town of Grande Cache Policy and Procedures Manual



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|--------------------------------------|
| Title | Guidelines for Acceptable Use of Communication Technology Resources | Page 1 of 4 |
| Section | FOIP/IT Security | Resolution No. 157/16 |
| Department | All | Effective Date April 13, 2016 |

The following guidelines are intended as examples and do not represent a complete list. If there are any questions, please speak with your immediate supervisor for clarification.

| Things to Do | Things NOT to Do |
|---|--|
| <p><i>Use for accomplishing job responsibilities that support vision, mission and value statements</i></p> <ul style="list-style-type: none"> ✓ Communicate with others in a respectful and professional manner ✓ Use footers (ie. privacy) only on appropriate content and with the approval of the Department Manager ✓ Obtain approval when borrowing or relocating any communication technology resources ✓ Clearly and accurately identify yourself when sending messages ✓ Communicate on another's behalf only with that individual's approval | <ul style="list-style-type: none"> ✗ Use involving illegal activities ✗ Access, communicate, distribute, or display racial or ethnic slurs, threats, insults, obscenities, abuse, defamation or sexually explicit material ✗ Communicate personal or confidential information without authorization ✗ Reveal or publicize protected information ✗ Share or reveal passwords without authorization ✗ Represent personal opinions as those of the Town (or department, etc.) |
| <p><i>Use for career or personal development, including professional networking subject to the Code of Conduct</i></p> <ul style="list-style-type: none"> ✓ Obtain approval for career or personal development, such as web-based training ✓ Communicate appropriately with external contacts ✓ Communicate personal and confidential information in a secure manner | <ul style="list-style-type: none"> ✗ Promote personal or private business ventures ✗ Send non-approved or non-work requests or notifications to Town group lists ✗ Send, copy, install or download copyrighted documents (this includes audio and visual files) ✗ Use confidential Town information for personal or non-work purposes |



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|--------------------------------------|
| Title | Guidelines for Acceptable Use of Communication Technology Resources | Page 2 of 4 |
| Section | FOIP/IT Security | Resolution No. 157/16 |
| Department | All | Effective Date April 13, 2016 |

| Things to Do | Things NOT to Do |
|--|---|
| <p>Personal use which is occasional or incidental and/or approved by my supervisor</p> <ul style="list-style-type: none"> ✓ Obtain approval for exemptions ✓ Reimburse the Town promptly for personal costs ✓ Personal use on non-work time or breaks | <ul style="list-style-type: none"> ✗ Use for personal gain or profit, including personal or private business activity ✗ Use communication technology resources for political or religious campaigning, or to promote activities or objectives of associations, clubs or unions ✗ Grant access to friends, family or any other persons ✗ Use communication technology resources for gambling, games, jokes or chain letters |
| <p>Use for maintaining the integrity of all Communication Technology Resources</p> <ul style="list-style-type: none"> ✓ Respect Town assets and take proper care of them ✓ Report any suspicious or unethical activity to your supervisor immediately ✓ Power off your device(s) at the end of each work day as often as your duties permit ✓ When away from your work area for extended periods, grant permission for access to the employee covering your job | <ul style="list-style-type: none"> ✗ Use that could cause congestion or disruption to normal operations of communication technology ✗ Tamper, alter, modify, reconfigure or change communication technology resources ✗ Engage in activities which are risky as to security or virus exposure, such as adjusting internal settings ✗ Install personal or unlicensed software ✗ Knowingly download or upload a virus or other malicious software ✗ Deliberately try to access information for which you are not authorized |



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|--------------------------------------|
| Title | Guidelines for Acceptable Use of Communication Technology Resources | Page 3 of 4 |
| Section | FOIP/IT Security | Resolution No. 157/16 |
| Department | All | Effective Date April 13, 2016 |

Frequently Asked Questions

- 1. I am taking an online course through NAIT which requires some research on the internet. Can I use my work computer for this purpose?**

Yes, provided that it is done on your own time without additional costs to the Town and that providing such research does not violate any provisions of the 'Acceptable Use of Communication Technology Resources' policy or the 'Employee Code of Conduct' policy.

- 2. Can I access my communication technology resource for occasional personal use? What about infrequent phone calls? Can I call my child's daycare or make a medical appointment?**

Yes. Incidental use of Town assets such as communication technology resources is allowed as long as there is no negative impact on your performance, no abuse of paid work time and/or no added costs to the Town. This includes telephone and cell phone use.

- 3. Can I photocopy recipes for distribution at my cooking class?**

Making one or two copies is not an abuse of Town assets. Multiple copies, however, require supervisor approval and reimbursement to the Town.

- 4. Can I use the internet at work to plan my vacation and book my airline tickets?**

Yes, provided that you do it on your own time (ie. lunch, coffee breaks) and there are no costs to the Town.

- 5. Can I install my personal income tax software on my work computer or laptop?**

No. Modification to any Town communication technology device requires approval from both your supervisor and the IT contractor.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|--------------------------------------|
| Title | Guidelines for Acceptable Use of Communication Technology Resources | Page 4 of 4 |
| Section | FOIP/IT Security | Resolution No. 157/16 |
| Department | All | Effective Date April 13, 2016 |

6. How can I protect my email account?

Lock your workstation when leaving it unattended ~ CTRL – ALT – DELETE, ENTER. Safeguard your password and do not share your email account.

7. Could the content of my email message be revealed in response to a FOIP request?

Yes. All email messages and attachments sent to and from your Town email account are Town records and subject to the Alberta FOIP Act.

8. Does the Town keep track of my computer use?

Yes. All computer use, from your Town email account for both personal and official Town business is monitored and logged. The logs are used for troubleshooting and to support investigations.

9. I find I am more productive if I work with some background music playing, is this okay?

When playing music at work, be mindful of the volume and content of the music and possible distraction to employees around your work space. Downloading music files on your computer is not allowed.

10. I need my computer moved to another location. Can I move it myself or do I have to inform whoever is in charge of IT of its new location?

Do not move computers until speaking to the IT contact person prior to relocation of hardware. Instructions will be provided either through the contact person or directly from the IT contractor.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices | Page 1 of 2 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

The Town of Grande Cache is committed to safe and responsible use of communication and technology resources to protect information collected and utilized in the daily operations of the Town. The Protection of Mobile Devices and Mobile Sensitive Data Policy protects the interests of the Town, users of the Town’s communication and technology resources and the public by providing a standard for the collection, use, storage and protection of information held in the custody of the municipality.

These Guidelines were developed to provide elected officials, employees and contractors with clear direction on expectations for the use and protection of Town mobile devices and mobile data storage devices.

Regular/Ongoing:

- ✓ When leaving work at the end of the day, secure all mobile data storage in lockable cabinets or drawers in your office or designated area.
- ✓ Regularly review the contents of mobile data storage to identify and erase sensitive data that is no longer required on the device. List the contents on the device and store it in a secure location (locked cabinet, safe, etc.) for quick reference if the device is lost or stolen.
- ✓ Regularly delete temporary electronic copies of any Town information that is no longer needed as directed in the Records and Information Management Program.
- ✓ Regularly check that you are still in possession of all mobile data storage, in order to identify as early as possible any assets that may have been lost or stolen.
- ✓ Regularly copy updated Town information back to the Town information banks.
- ✗ NEVER keep the only copy of any data or document on mobile data storage



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices | Page 2 of 2 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

Sensitive Data Located on Mobile Data Storage

- ✓ Always store mobile sensitive data using an encryption solution ~ a login password is not enough. Where possible, store mobile sensitive data on mobile data storage which comes with built-in encryption solutions.
- ✓ It is prohibited for employees to disable or attempt to disable encryption solutions.
- ✓ Keys or passwords used with encryption solutions must be recorded and kept in a secure location and only communicated to others allowed access to the information.

Prior to Transporting Mobile Data Storage Outside of Town Premises

- ✓ Mobile data storage must not be labeled with any identifier which would identify it as owned by the Town of Grande Cache. Either have no label or use a phone number.
- ✓ When travelling with mobile data storage, secure the device(s) in a lockable trunk or storage compartment in the vehicle when possible.
- ✗ NEVER leave mobile data storage in a motor vehicle.

While Mobile Data Storage is Outside of Town Premises

- ✓ Keep mobile data storage with you at all times when travelling on foot in public places. This includes going into restaurants and washrooms and while shopping.
- ✓ Always bring mobile data storage with you as carry-on luggage when travelling on airlines, trains, buses or other public transportation.
- ✗ NEVER leave mobile data storage unattended, take it with you or in the care of a Town employee travelling with you.



TOWN OF GRANDE CACHE Policy and Procedures

Title Information Access and Security - Physical, Electronic and Remote Page 1 of 9

Section FOIP/IT Security **Resolution No.** 304/16
Department All **Effective Date** June 8, 2016

P

Background

The Town of Grande Cache recognizes the importance of its employees, in the performance of their duties, to be able to access information and communicate with each other and other stakeholders in a timely and efficient manner. Records and information in the possession of Town employees are assets that require management to ensure they serve both current operational purposes and potential legal and historical purposes.

O

1.0 Policy Statement

The Town of Grande Cache shall employ physical, administrative and technical access controls at all facilities for areas containing information, information processing and storage and information technology (IT) resources. These controls may include, but are not limited to alarms, access codes, staffed reception desks, unique User ID's and passwords.

L

2.0 Purpose

The purpose of this policy is to ensure the Town of Grande Cache employs consistent physical, administrative and technical access controls to safeguard employees and the public, and to protect the security of information and information technology resources, including information processing and storage equipment and facilities.

I

C

3.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

Y



TOWN OF GRANDE CACHE
Policy and Procedures

Table with 2 columns: Title (Information Access and Security - Physical, Electronic and Remote) and Page (2 of 9). Row 2: Section (FOIP/IT Security), Department (All), Resolution No. (304/16), Effective Date (June 8, 2016).

Communication and Information Technology (IT) Resources that is any means by which information is exchanged between individuals through a common system, which includes, but is not limited to:

- a) computers (desktop, portable and wireless computing devices);
b) mobile computing devices (notebook computers, laptops, tablets, cell phones, smart phones), air cards, push to talk radios and modems;
c) internet and electronic communication services (email, instant messenger, voice mail, long distance and roaming, voice/text/data transmission, etc.);
d) network infrastructures (ie. fiber optics cables, wireless networks, wi-fi access, etc.);
e) photocopiers, fax machines, printers, scanners, cameras, radios, televisions, audio/visual equipment and desktop telephones;
f) business systems, office productivity systems, utility and all other Town-administered systems and related server and storage infrastructure;
g) consumable goods used in the operation of these resources (DVD's, CD's, tape media, paper, USB memory sticks, etc.); and
h) all data, information online services and software applications which can be accessed using the above mentioned, including electronic mail, internet and chat technologies.

Communication and Information Technology Resource Users includes but is not limited to Town of Grande Cache employees, vendors, contractors, consultants and any other individuals with authorized access to and use of the Town IT resources.

Confidential means the classification applied to information where the unauthorized disclosure could cause moderate risk or harm to any individual, the Town or third party, or to the privacy of individuals, compromise the business interests of a third party, or threaten the secure containment of privileged information or records.

Contractor is any affiliate, third party, non-employee, consultant or agent or employee of a contractor or service provider engaged by the Town to perform services for or on behalf of the Town.

Data is a general term used to denote any or all facts, numbers, letters and symbols that refer to or describe an object, idea, condition, situation or other factors in a computerized form.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 3 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

Department is an internal administrative division of the Town including all Town offices.

Designated Security Officer means the individual(s) designated by the Chief Administrative Officer and has the responsibility to manage, monitor and control the physical security of information, information processing and storage equipment and facilities.

Encryption Solution means Town-approved technical solutions for converting information into unreadable forms (via industry standard methods) which are essentially impossible to translate back into readable form without using the correct original encryption key.

FOIP Act means the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 as amended.

Information means any information that identifies an individual or business and is stored in any format that the Town utilizes in the usual business operations of the municipality.

IT Resource means any Town-owned or controlled asset used to generate, process, transmit, store or access Town information.

IT Resource Officer means the individual designated by the Chief Administrative Officer and has the responsibility to manage and control communication and technology resources for the Town.

Log means an electronic or written record of a network, application or system's activity used for information, backup, recovery or review.

Personal Information is recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number, the individual's age, sex, marital or family status, information about the individual's educational, financial, employment or criminal history, etc.

(for a complete definition, refer to section 1 (n) of the FOIP Act)



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 4 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

Record means a collection of information in any form and includes notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records (for a complete definition, refer to s. 1 (q) of the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended);

Remote Access means a Town-approved method of electronically accessing data from Town Information Banks from outside of Town premises via remotely connecting and communicating with the Town system. This includes but is not limited to Outlook Web Access or other network solution approved by the Town.

Secure Area means any area in a Town facility where access is restricted to authorized personnel to protect sensitive Town assets, including IT resources.

Town Assets means all property legally or beneficially owned by the Town, including equipment, financial assets, land, buildings, vehicles, material, communication technology, information and intangible property.

User means any person authorized to access and/or use Town IT resources.

4.0 Policy Guidelines and Principals

4.1 Scope

This policy applies to all Town officials, employees and contractors (hereinafter referred to as 'Users') whose access to or use of information and/or records and information technology resources that is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town's premises or elsewhere.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 5 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

4.2 Responsibility for Physical Access to Information

The Chief Administrative Officer is responsible:

- a) for the management of physical access control and security;
- b) to establish designated contacts ('designated security officer') for physical access control and authorization for access requests, keys, access codes or other physical access control measures;
- c) review Town facility access rights for Users regularly;
- d) to designate an officer of the Town to conduct a physical security assessment of all facilities and equipment periodically to ensure applicable security measures comply with Town policy for information security and access; and
- e) to ensure all employees and other persons acting on behalf of the town shall take reasonable precautions to ensure Town IT resources are in secure areas that minimize potential risks from unauthorized access, security threats and environmental hazards.

4.3 Physical Access Controls

- 4.3.1 Information processing and storage devices shall be located in secure areas and protected by entry controls to protect against unauthorized access, damage, theft and interference.
- 4.3.2 Any staff aware of a potential or actual threat or breach to the integrity of a physical access control shall report the threat or breach to the designated security officer immediately. The designated security officer shall complete and submit an incident report about the potential or actual threat or breach to Chief Administrative Officer.
- 4.3.4 Contact information for the designated security officer shall be provided to all staff and applicable contractors at all Town facilities.

4.4 Electronic Information Access

- 4.4.1 Access to Town information will only be granted if such access is necessary to fulfill authorized Town duties and responsibilities. Access shall be to the minimum information necessary to perform the duties and responsibilities of that individual.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 6 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

4.4.2 Requests for employee electronic access shall be submitted to the designated officer for IT resources ('IT Resources Officer'). A User access profile will be created and information access privileges will be granted based on the role and responsibilities of the User.

4.4.4 The IT Resources Officer is responsible:

- a) to grant access to information and IT resources to the level required to perform specific role-related duties and responsibilities;
- b) to ensure all Users are assigned a personal and unique User ID and password;
- c) to review User access rights, either as part of a routine security review or as required, and has the authority to revoke or modify privileges when necessary and ensure a password management process for granting access to IT resources;
- d) to ensure that the IT contractor reviews and investigates any unusual access activities and submit a report immediately to the IT resources officer for further investigation or action(s); and
- e) if the IT resources officer deems there is a potential or actual threat or breach, it will be immediately reported to the Chief Administrative Officer.

4.5 Management of Electronic Information Access

4.5.1 The IT resources officer shall control and limit access to authorized Users for software applications, databases, internal and external networks and shared-file drives.

4.5.2 No user of the Town's communication and IT resources should assume or operate under another user's electronic identity.

4.5.3 Each User is responsible for all actions performed under their User ID log-in. Users shall take the necessary security precautions to prevent User ID misuse. Users will not share or transfer passwords and User ID's to any other person. Users are individually responsible for updating and safeguarding their passwords.

4.5.4 Passwords should not be shared or revealed, this includes family and other household members when work is being done at home. Keep passwords secure and do not share user accounts. Authorized users are responsible for the security of their passwords and accounts.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 8 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

4.7.2 All PC's, laptops and workstations are to be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device is left unattended. Because information contained on mobile devices is especially vulnerable, users must follow the 'Protection of Mobile Devices and Mobile Data Storage Devices' policy and guidelines to protect access to the device.

4.7.2 Employees assigned mobile devices or mobile data storage devices must secure all mobile devices in lockable cabinets or drawers in your office or designated area.

4.7.3 All sensitive data should be stored using a Town-approved encryption solution ~ a login password is not enough.

4.7.4 All sensitive data on mobile data storage devices should be stored using a Town-approved encryption solution and must be secured in designed location (locked cabinet, safe, etc.).

4.7.5 It is prohibited for employees to disable or attempt to disable encryption solutions.

4.7.6 Keys or passwords used with encryption solutions must be recorded and kept in a secure location and only communicated to others allowed access to the information.

4.8 Termination of Employment, Agreement, Contract or Appointment

4.8.1 All physical access privileges shall be revoked immediately upon expiration or termination of an individual's employment, agreement, contract, service or appointment with the Town. All access codes and/or keys must be immediately returned to the immediate supervisor, department manager or designated security officer.

4.8.2 Supervisors or managers shall contact the IT resource officer to remove the individual's access privileges. The IT resource officer shall ensure all electronic access privileges, including disabling email accounts, are revoked upon termination of an individual's employment, contract, service or appointment with the Town.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|------------------------------------|
| Title | Information Access and Security - Physical, Electronic and Remote | Page 9 of 9 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

4.8.3 If an employee transfers to a different position or department, the IT resource officer shall ensure all access privileges are adjusted to reflect the new position or department access requirements.

4.9 Contractor Access

Any contractor granted access to deal with Town information or IT resources shall comply with Town IT Security policies both inside and outside of Town facilities. Staff responsible for negotiating, administering and managing Town contracts shall ensure that all access provisions are met and adhered to.

5.0 Compliance

- 5.1 Employees must report suspected violations or fraudulent activities to their immediate supervisor and/or department manager. Suspected violations that involve criminal conduct must be reported immediately to the Chief Administrative Officer or designate.
- 5.2 Any violation of this policy may subject the employee to their loss of access to records and use of communication and technology resources, and may result in disciplinary actions being taken, up to and including dismissal from employment.
- 5.3 Illegal acts involving communication and technology resources may also subject the user to restitution, commencement of civil action, or criminal investigation and prosecution by police agencies and/or local, provincial and federal authorities.



TOWN OF GRANDE CACHE
Policy and Procedures

Table with 2 columns: Information and Records Management, Page 1 of 7. Rows include Section (FOIP/IT Security), Department (All), Resolution No. (304/16), and Effective Date (June 8, 2016).

P

Background

The Town of Grande Cache recognizes the importance of a systematic approach to the management of corporate information and records which is essential for the Town to protect and preserve corporate information and records as evidence of actions to support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders.

O

1.0 Purpose

1.1 The purpose of this policy is to:

- a) achieve efficient and effective records and information management to capture, manage, share, store, preserve and deliver all corporate records, regardless of media, in a system capable of supporting municipal functions and program and service delivery;
b) foster informed decision-making;
c) facilitate accountability, transparency and collaboration; and
d) ensure the disposition of corporate records is done in accordance with the Management of Municipal Records Bylaw.

L

2.0 Policy Statement

An efficient and economical information and records management program assures the systematic control and management of information as a corporate asset. The Town will maintain a uniform process which will assure the availability of information required in the management of operational activities, protect legal rights, ensure statutory compliance, support tax and audit requirements and ensure the availability of essential information for the resumption of operations following a disaster.

I

C

3.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

Y



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Information and Records Management | | | Page 2 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

Collection occurs when a public body gathers, receives or obtains personal information. This includes activities where individuals respond through interviews, questionnaires, surveys, polling, or by completing forms in order to provide information to public bodies. The means of collection may be in writing, electronic data entry or other such means.

Data is a general term used to denote any or all facts, numbers, letters and symbols that refer to or describe an object, idea, condition, situation or other factors in a computerized form.

Department is an internal administrative division of the Town including all Town offices.

Disposition means the destruction of records or the transfer of records of enduring value to the Town archives.

FOIP Act means the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 as amended.

Information means any data that identifies an individual or business and is stored in any format that the Town utilizes in the usual business operations of the municipality.

Life Cycle of Records means the lifespan of a record from its creation or receipt through its active, semi-active and inactive stages, to its disposition.

Municipal Information and Records Management Program (the 'Program') means the system developed by the Town to manage and administer municipal records in an efficient, effective and consistent manner throughout the organization in accordance with all applicable legislation.

Personal Information is recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number, the individual's age, sex, marital or family status, information about the individual's educational, financial, employment or criminal history, etc.
(for a complete definition, refer to section 1 (n) of the FOIP Act)

Public Body for the purpose of this policy, is defined in section 1 (p) of the FOIP Act and includes the Town of Grande Cache.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|---|-----------------------|--------------|
| Title | Information and Records Management | | Page 3 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

Record means a collection of information in any form and includes notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records (for a complete definition, refer to s. 1 (q) of the *Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended*);

Records Management is the application of systematic control over records throughout their life cycle, including but not limited to the management of forms, manuals, records inventory, file systems development and implementation, file maintenance procedures development, file equipment selection, correspondence and reports maintenance and records scheduling and disposition.

Retention Schedule is the approved document which authorizes the length of time active and semi-active records are to be maintained, the medium in which they are to be preserved and the method of disposition.

3.0 Policy Guidelines and Principles

3.1 Scope

This policy applies to all Town officials, employees and contractors (hereinafter referred to as ‘Users’) whose access to or use of information and/or records and information technology resources that is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town’s premises or elsewhere.

3.2 Records of the Municipality

3.2.1 All corporate records that are created, received and used in the conduct of Town business activities contain information that is a valuable resource and are important business assets that are the property of the Town of Grande Cache.

3.2.2 Records under the control of the Town, including all departments, both records municipal operations and actions and preserves the Town’s history. Municipal records supports public reporting, sound planning and decision-making for current and future governments.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Information and Records Management | | | Page 4 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.2.3 Records are retained:

- a) to support municipal business operations;
- b) as proof of business transactions;
- c) to comply with legislation;
- d) to protect the rights of citizens and the Town;
- e) as proof of accountability and compliance with other business requirements; and
- f) for future business, financial, legal, research or archival reference.

3.3.4 Hard copy paper records and electronic data are standard information mediums in municipalities. Some information is more sensitive than others and may contain personal information which must be protected regardless of the format. Management shall actively support personal information security with the municipality through clear direction, demonstrated commitment, explicit assignment and acknowledgement of personal information security responsibilities.

3.3.5 Because municipal records are a valuable asset, they must be treated as such and is the responsibility of all employees.

3.3 Objectives

3.3.1 Municipal records are managed to meet requirements for the Town as a whole, including:

- a) what information and records are collected;
- b) who has access to specific records;
- c) how the records are used;
- d) how records are classified, organized and stored; and
- e) identifying and determining the specific requirements for departmental operational needs and accountabilities.

3.3.2 The expected results of this policy are to ensure:

- a) municipal functions, programs and services provides convenient access to reliable, comprehensive information in a timely manner;
- b) information and records are managed as valuable assets to support municipal functions and operational needs and accountabilities; and
- c) that structures, mechanisms and resources are in place to ensure the continuous and effective management of information.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Information and Records Management | | | Page 5 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.4 Information and Records Technology

Efficient and effective information and records technology is a key enabler to achieving well-managed records in support of policies, services and programs.

3.5 Stewardship and Security

3.5.1 Municipal records must be rigorously managed throughout their lifecycle, regardless of medium or format, for as long as the record is required to meet operational and fiscal responsibilities, legal obligations and accountabilities. This means that procedures are in place to ensure records are current, complete and accurate.

3.5.2 Ensuring the confidentiality, integrity and availability of records is essential to municipal decision-making and the delivery of services. Effective security of records requires a systematic approach that identifies and categorizes information and associated assets, assesses risk and implements personnel, physical and IT safeguards.

3.6 Access and Privacy

Respect for individual privacy applies across the records lifecycle in accordance with the FOIP Act. It is the responsibility of each employee to be aware of and comply with the FOIP Act and Regulations, Town policies and other related legislation with regard to information and records access and protection of privacy.

3.7 Transparency

Employees document actions and decisions in support of Town services, activities and programs, and maintain information and records so that it is accessible to anyone who is authorized to have access, including those individuals exercising their rights to access information under the FOIP Act. Managing information to support transparency and accountability also means reporting on performance in ways that are clear to citizens and Council.

3.8 Responsibility

Municipal records management, including retention and destruction, is the responsibility of the CAO or designate.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Information and Records Management | | | Page 6 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.9 Retention

3.9.1 Generally, there are four reasons for retaining records:

- a) **Administrative Value** – records have value to the Town if they assist in the performance of current or future activities. Normally, these records lose their value shortly after completion of their activity, therefore the retention time would be less (ie. routine response to an inquiry).
- b) **Legal Value** – the value of these documents usually does not diminish over a period of time. These documents are usually required by legislation (ie. meeting minutes, bylaws, etc.).
- c) **Fiscal Value** – these records relate to financial transactions such as financial ledges, debenture records, audit files, budgets, etc.
- d) **Research/Historical Value** – records that may contain information on persons, places, events, history or the development of the Town and its citizens.

4.0 Municipal Information and Records Management Program

4.1 Employees are required to manage records in any medium in accordance with the direction of the Program. This includes the timely and proper identification and classification of corporate records, the storage of those records in the appropriate systems, including electronic systems, and regular identification and destruction of transitory records.

4.2 The Chief Administrative Officer or designate is responsible for providing direction and leadership in the Program. This includes the development, implementation and monitoring of all Program components which defines information and records management requirements for the Town.

4.3 The Chief Administrative Officer or designate will:

- a) manage the Program to ensure it is administered according to all relevant legislation;
- b) ensure that records are managed and tracked throughout their entire lifecycle regardless of the medium in which they exist; and



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Information and Records Management | | | Page 7 of 7 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

c) ensure that the content of the records can be trusted as accurate representation of the business transaction.

4.4 The Chief Administrative Officer or designate will ensure that an appropriate storage environment for all records media which provides access, retrieval, protection and disposition of those records.

4.5 The Chief Administrative Officer or designate will provide guidance and support for the Program to all departments and will conduct regular reviews to ensure compliance with the Program.

5.0 Compliance

5.1 Employees must report suspected violations or fraudulent activities pertaining to municipal records to their immediate supervisor and/or department manager.

5.2 Suspected violations that involve criminal conduct must be reported immediately to the Chief Administrative Officer or designate.

5.3 Any violation of this policy may subject the employee to their loss of access to records and use of communication and technology resources, and may result in disciplinary actions being taken, up to and including dismissal from employment.

5.4 Illegal acts involving communication and technology resources may also subject the user to restitution, commencement of civil action, or criminal investigation and prosecution by police agencies and/or local, provincial and federal authorities.



TOWN OF GRANDE CACHE
Policy and Procedures

Title Internet and Email Use Page 1 of 6

Section FOIP/IT Security Resolution No. 304/16
Department All Effective Date June 8, 2016

P

Background

The Town of Grande Cache (the 'Town') is committed to safe and responsible use of communication and technology resources to protect the interests of the Town and ensure responsible use of taxpayer dollars.

O

1.0 Purpose

The purpose of this policy is to establish guidelines governing acceptable use of the Town's internet and email resources and in support of the 'Information Access and Security – Physical, Electronic and Remote' policy and Guidelines.

L

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

I

Contractor is any affiliate, third party, non-employee, consultant or agent or employee of a contractor or service provider engaged by the Town to perform services for or on behalf of the Town.

C

User means any person authorized to access and/or use Town communication and technology resources.

Y

All other terms referred to in this policy are as defined in the 'Information Access and Security – Physical, Electronic and Remote' policy.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|-------------------------------|-----------------------|--------------|-------------|
| Title | Internet and Email Use | | | Page 2 of 6 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.0 Policy and Guidelines

3.1 Scope

This policy applies to all Town officials, employees, guests and contractors (hereinafter referred to as ‘Users’) whose access to or use of internet and email resources is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town’s premises or elsewhere.

3.2 Objectives

With the Town establishing and maintaining compliance with this policy, the benefits of these communication tools can be realized, while the risks and costs are mitigated. The objectives of this policy are to ensure that:

- a) use of the Town’s internet and email resources are for the benefit of the Town;
- b) users understand that email messages and documents may be subject to the same laws, regulations, policies and other requirements as information communicated in other written forms and formats;
- c) disruptions to the Town’s activities from inappropriate use of the Town’s internet and email services are avoided; and
- d) Users are provided guidelines describing their personal responsibilities regarding confidentiality, privacy and acceptable use of the Town’s internet and email as defined by this policy and other applicable Town policies.

3.3 Principles of Acceptable Use

3.3.1 As with any resource provided by the Town, internet and email resources should be dedicated to legitimate Town business activities and governed by rules of conduct similar to those applicable to the use of other information technology resources. The use of internet and email resources imposes certain responsibilities and obligations on all Users and is subject to the Town’s policies and procedures and all provincial and federal laws.

3.3.2 Acceptable use must be legal and ethical. Acceptable use demonstrates respect for intellectual property, ownership of information, network system security mechanisms and individual’s rights to privacy and freedom from intimidation, harassment and unwarranted annoyance.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | |
|-------------------|-------------------------------|-----------------------|--------------|
| Title | Internet and Email Use | Page | 3 of 6 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

3.3.3 Furthermore, the nature of email raises expectations for a timely response – Users are urged to read and respond to all emails in a prompt and courteous manner.

3.3.4 All internet and email use shall:

- a) respect and uphold the law, including provincial and federal laws and regulations and the laws of other jurisdictions;
- b) comply with the Town’s stated policies, procedures, standards and guidelines;
- c) be courteous and follow accepted standards of etiquette;
- d) protect others’ privacy and confidentiality;
- e) reflect responsible use of internet and email resources;
- f) use information technology resources efficiently and productively; and
- g) contain a clause that claims the User’s confidentiality over the contents of any communication.

3.4 Acceptable and Unacceptable Activities

3.4.1 Acceptable internet and email activities are those that conform to the purpose, vision, mission and key principles of the Town and to each User’s job duties and/or responsibilities. The following list, including but not limited to, provides examples of **unacceptable** uses:

- a) engaging in any illegal activity or using the Town’s resources for any illegal purpose;
- b) knowingly disseminating harassing, abusive, malicious, sexually explicit, threatening or illegal information, including jokes or cartoons;
- c) using the Town’s resources for purposes unrelated to the Town’s business activities, such as personal commercial use, advertisements, solicitations or promotions;
- d) using the Town’s resources to send messages expressing controversial, potentially offensive and/or defamatory comments of individuals, bodies corporate or groups including but not limited to, religion, politics and social policies;
- e) downloading or using the material, software or other intellectual property of others in violation of software licenses, copyright and trademark laws;
- f) disclosing any passwords or security means and methods adopted by the Town; and
- g) downloading or using any software not approved for use by the Town.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|-------------------------------|-----------------------|--------------|
| Title | Internet and Email Use | Page | 4 of 6 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

3.4.2 Users may use the Town’s internet and email resources for incidental and occasional personal use, provided that such use is reasonable in duration, does not take place during normal work hours (excluding coffee or lunch breaks), does not result in increased costs to the Town and complies with this and all other Town policies.

3.5 Privacy and Monitoring

3.5.1 Files in User’s accounts and data on the network are regarded as personal ~ that is, the Town does not routinely monitor this information. However, the Town reserves the right to view or scan any file, email or software stored on the Town’s systems or transmitted over the Town’s networks and may do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses or unauthorized software), or to audit the use of the Town’s resources. Potential violations of this policy that come to the Town’s attention during these and other activities may be acted upon.

3.5.2 Users must not send email messages containing unusually sensitive information over the internet without using an encryption method approved by the Town. The Town must be provided with a copy of all passwords and/or private key needed to decrypt the communications.

3.5.3 Users must recognize that electronic correspondence is not inherently private, that messages could be misdirected and that the Town takes no responsibility resulting from the disclosure of private communications occurring over the Town’s resources.

3.5.4 Users are reminded that if they do not want anyone to read about anything from a communication, they should not put it in an email.

3.5.5 Users are advised to remove themselves from internet and email lists not dealing with work-related topics.

3.5.6 The Town reserves the right to monitor, access, investigate and audit any and all electronic communications and use of the internet to ensure the integrity of the system and compliance with this and all other Town policies.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|-------------------------------|-----------------------|--------------|
| Title | Internet and Email Use | Page | 6 of 6 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

4.0 **Compliance**

- 4.1 Employees must report suspected violations or fraudulent activities to their immediate supervisor and/or department manager. Suspected violations that involve criminal conduct must be reported immediately to the Chief Administrative Officer or designate.

- 4.2 Suspected violations of this policy may result in suspension of the User’s access to the Town’s internet and email resources, followed by a review of any costs and/or charges incurred by the Town.

- 4.3 Any violation of this policy may subject the User to their loss of internet and email access privileges and use of communication and technology resources, and may result in disciplinary actions being taken, up to and including dismissal from employment.

- 4.4 Illegal acts involving internet and email use may also subject the user to restitution, commencement of civil action, or criminal investigation and prosecution by police agencies and/or local, provincial and federal authorities.

| | | | |
|--|---|--------------------------------------|--------|
| POLICY AND PROCEDURE MANUAL | Subject Municipal Emergency Management | Section No. X-1 | Page 1 |
| | Department Emergency Management | Approved by Resolution No. 025/13 | |
| | Effective Date January 23, 2013 | Supersedes | |

MUNICIPAL EMERGENCY MANAGEMENT POLICY

Background

In accordance with CSA Z1600-08, Municipal Emergency Management should be based on a policy that includes a vision, mission statement, roles and responsibilities and enabling authority. The policy should be approved by the executive, which is the local authority.

Risk

Without a clear policy statement as the foundation for the overall Municipal Emergency Management framework, the Municipal Emergency Management Agency will lack direction and the necessary authority to carry out their emergency management functions of prevention, planning, response and recovery.

Recommended Policy

Vision

To make the Town of Grande Cache a safe and secure place for residents, businesses and visitors during any emergency or disaster.

Mission Statement

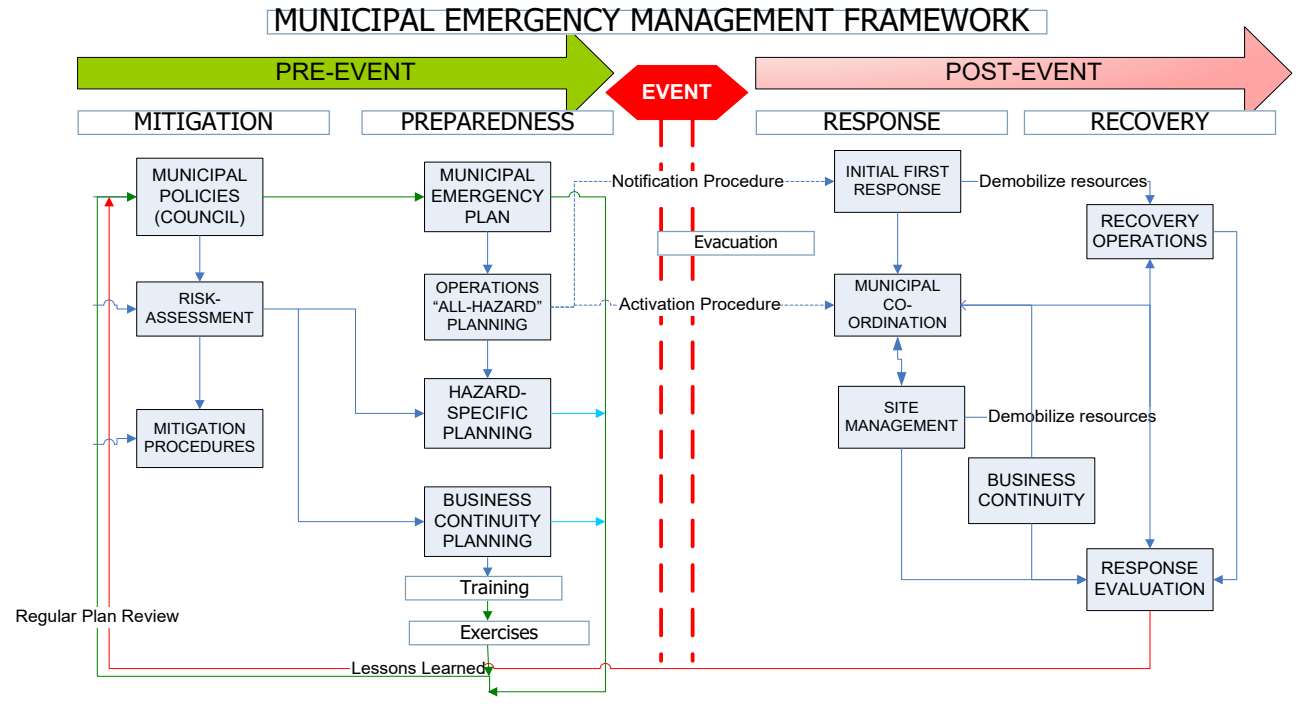
To achieve emergency management capacity in the Town of Grande Cache for the prevention, planning, response and recovery of all emergencies in a pro-active, operations-focused manner, based on standards, policies and continuous improvement in cooperation and coordination with all stakeholders and partners.

Roles and Responsibilities

Under the leadership and guidance of Council, the Town of Grande Cache will establish and maintain a Municipal Emergency Management Agency that defines the goals and objectives of the municipal emergency management program and creates and maintains plans and procedures based on hazard-analysis to achieve the mission statement objectives in coordination and cooperation with neighbors, industry and agencies that are active in the municipality.

| | | | |
|--|---|--------------------------------------|--------|
| POLICY AND PROCEDURE MANUAL | Subject Municipal Emergency Management | Section No. X-1 | Page 2 |
| | Department Emergency Management | Approved by Resolution No. 025/13 | |
| | Effective Date January 23, 2013 | Supersedes | |

Framework Programs



Record Management

The Town of Grande Cache will establish and maintain records to demonstrate conformity with the program administration requirements and to document the effective operation of the emergency management and business continuity programs. Records will be legible, readily identifiable and retrievable. Procedures will be established to define the controls required for the identification, secure storage, protection, retrieval, retention time and disposition of records.

Records can include those kept for:

- the implementation of the emergency management and business continuity programs;
- events and actions taken to mitigate, prepare for, respond to and recover from an incident;
- legal requirements;
- training and monitoring activities, including the results of monitoring;
- changes or improvements made to prevention, mitigation, preparedness, response and recovery strategies.

Privacy legislation, industry codes of practice and guidelines will also be considered.

(ref: CSA Z1600-08)

| | | | |
|--|--|--------------------------------------|--------|
| POLICY AND PROCEDURE MANUAL | Subject Notification of Emergencies | Section No. X-1 | Page 5 |
| | Department Emergency Management | Approved by Resolution No. 028/13 | |
| | Effective Date January 23, 2013 | Supersedes | |

MUNICIPAL NOTIFICATION OF EMERGENCIES POLICY

Background

Municipal notification is the process of communicating to the municipality information regarding emergency events that may require additional considerations beyond first response procedures in order to ensure early and proactive emergency management coordination. When an emergency is anticipated, or an emergency occurs, agencies (typically first responders) arriving at the site should assess if the Municipal Director of Emergency Management (DEM) needs to be informed of the emergency. This assessment should be based on established operational criteria resulting in the applicable notification decision.

Risk

The lack of clearly communicated notification procedures could result in failure to activate the Municipal Emergency Coordination Procedures in a timely manner. This failure to activate the emergency procedures could prevent the municipality from supporting the incident response as required and protecting public safety, property and the environment. The procedure and criteria for notification must be clear and communicated effectively to all agencies operating in the municipality. The notification procedure forms part of the Municipal Emergency Management Plan and must be included in training and exercises.

Recommended Policy

To ensure timely and effective emergency management in the Town of Grande Cache, municipal notification of emergencies shall be proactive, based on event criteria and developed as part of the Municipal Emergency Management Plan. The notification procedures shall be communicated to all municipal, regional and contracted agencies operating in the municipality, including those with the potential of responding to an emergency or those who may become aware of an emergency. The Director of Emergency Management shall establish, distribute and exercise these municipal notification procedures as part of the Municipal Emergency Management Plan.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | | |
|-------------------|-----------------------|-----------------------|--------------|-------------|
| Title | Privacy Breach | | | Page 1 of 4 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

P

Background

The Town of Grande Cache (the 'Town') is committed to safe and responsible collection and use of personal information and to ensure the Town employs consistent access controls to safeguard and protect the security of information and information technology resources.

O

1.0 Purpose

The purpose of this policy is to establish the procedures and guidelines for reporting a breach of privacy.

L

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

I

Department is an internal administrative division of the Town including all Town offices.

C

Disclosure means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give personal information by any means to someone. This includes oral transmission of information by telephone, or in person, provision of personal information on paper, by facsimile or in another format, and electronic transmission through electronic mail, data transfer or the internet.

FOIP Act means the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended.

Y

Personal Information is recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number, the individual's age, sex, marital or family status, etc.

(for a complete definition, refer to section 1 (n) of the FOIP Act)



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|-----------------------|-----------------------|--------------|
| Title | Privacy Breach | Page | 2 of 4 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

Privacy Breach occurs when personal information is collected, retained, used or disclosed in ways that are contrary to the provision of the FOIP Act. A common breach of personal privacy is the unauthorized disclosure of personal information, contrary to Section 40 of the FOIP Act.

Levels of a Breach are defined as:

Low Level ~ basic personal information, such as name, picture, date of birth or salary, which the release of, while causing annoyance and inconvenience, is unlikely to result in significant lasting harm
~ involves Town employees and the release of personal information occurs internally (within the Town of Grande Cache only)
~ a release of personal information of a non-employee or an external breach moves the breach level to medium

Medium Level ~ sensitive personal information, including but not limited to, personnel records, minor health information or financial records that may result in significant harm
(ie. a page from a Human Resources file)

High Level ~ comprehensive, detailed personal information, such as banking records, social insurance number, payroll information, detailed health information, family information, etc.
~ usually typified by the release of a significant amount of personal information or involves a large number of individuals

Public Body for the purpose of this policy, is defined in section 1 (p) of the FOIP Act and includes the Town of Grande Cache.

3.0 Policy Guidelines and Principals for Responding to a Privacy Breach

3.1 **Scope**

This policy applies to all Town officials, employees and contractors (hereinafter referred to as 'Users') whose access to or use of information and/or records and information technology resources that is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town's premises or elsewhere.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | |
|-------------------|-----------------------|-----------------------|--------------|
| Title | Privacy Breach | Page | 3 of 4 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

3.2 What is a Privacy Breach?

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is 'unauthorized' if it occurs in contravention of the FOIP Act. Common privacy breach happens when personal information of customers or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or when personal information is emailed to the wrong person by mistake.

3.3 Responding to a Privacy Breach

- 3.3.1 When a privacy breach has been discovered, immediate action must be taken. Please refer to the 'Key Steps in Responding to a Privacy Breach' for detailed actions in responding to a privacy breach.
- 3.2.2 Employees are expected to report a privacy breach to their supervisor when it is discovered.
- 3.2.3 Supervisors will confirm that a breach has occurred and will complete Section 1 of the 'Privacy Breach Report' form and provide a copy to the FOIP Coordinator.
- 3.2.4 The level of seriousness of the breach (high, medium or low) will be determined by the supervisor, department manager and FOIP Coordinator (Section 2 - Privacy Breach Report form).
- 3.2.5 Supervisors are responsible for preventing further breaches of the information within 24 hours of notification, including retrieval of records from an unauthorized recipient.
- 3.2.6 In the case of medium and high breaches, the FOIP Coordinator will contact the CAO, who will determine who is responsible to notify any individuals affected.
- 3.2.7 The FOIP Coordinator will contact the CAO, who will determine whether or not to notify the individuals affected by a low level breach.
- 3.2.8 The FOIP Coordinator is the primary contact with and will notify the Office of the Information and Privacy Commissioner of a privacy breach when necessary.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|-----------------------|------------------------------------|
| Title | Privacy Breach | Page 4 of 4 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

3.2.9 In the event of a high level breach, the CAO and/or the FOIP Coordinator will lead the official investigation.

3.3 Elected Officials

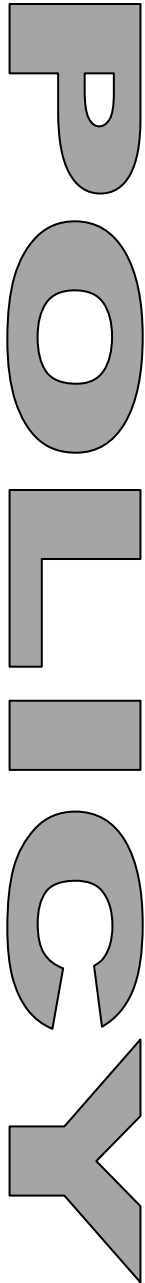
3.3.1 In the case where an elected official discovers a privacy breach, that individual must immediately notify the CAO or designate. The CAO or designate will confirm the privacy breach.

3.3.3 If there is a privacy breach, the CAO will determine what level of privacy breach occurred and decide what course of action to take, including prevention of further breach of information, notification of any affected individuals, retrieval of information or an official investigation.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | | |
|-------------------|--|-----------------------|--------------|-------------|
| Title | Protection of Information and Privacy | | | Page 1 of 5 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |



Background

The Town of Grande Cache (the 'Town') is committed to safe and responsible use of information and information technology resources to ensure the Town employs consistent physical, administrative and technical access controls to safeguard and protect the security of information and information technology resources.

1.0 Purpose

Within the limits required by law, this policy provides persons with specific levels of control over the Town's collection, use, disclosure and storage of personal information.

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

Collection occurs when a public body gathers, receives or obtains personal information. This includes activities where individuals respond through interviews, questionnaires, surveys, polling, or by completing forms in order to provide information to public bodies. The means of collection may be in writing, electronic data entry or other such means.

Data is a general term used to denote any or all facts, numbers, letters and symbols that refer to or describe an object, idea, condition, situation or other factors in a computerized form.

Department is an internal administrative division of the Town including all Town offices.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | |
|-------------------|--|-----------------------|--------------|
| Title | Protection of Information and Privacy | | Page 2 of 5 |
| Section | FOIP/IT Security | Resolution No. | 304/16 |
| Department | All | Effective Date | June 8, 2016 |

Disclosure means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give personal information by any means to someone. This includes oral transmission of information by telephone, or in person, provision of personal information on paper, by facsimile or in another format, and electronic transmission through electronic mail, data transfer or the internet.

FOIP Act means the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended.

Information means any data that identifies an individual or business and is stored in any format that the Town utilizes in the usual business operations of the municipality.

Personal Information is recorded information about an identifiable individual, including the individual’s name, home or business address or home or business telephone number, the individual’s age, sex, marital or family status, information about the individual’s educational, financial, employment or criminal history, etc.
(for a complete definition, refer to section 1 (n) of the FOIP Act)

Public Body for the purpose of this policy, is defined in section 1 (p) of the FOIP Act and includes the Town of Grande Cache.

Private Impact Assessment means a process that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of personal information may affect the privacy of the individual who is the subject of the information.

Record means a collection of information in any form and includes notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records *(for a complete definition, refer to s. 1 (q) of the Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended);*

Use of Personal Information means employing collected information to accomplish the public body’s purposes. For example, using the information to administer a program or activity, to provide a service or to determine eligibility for a benefit. Access to a file or database by program staff or contract agents is ‘use’ as defined under the FOIP Act.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|--|-----------------------|--------------|-------------|
| Title | Protection of Information and Privacy | | | Page 3 of 5 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.0 Policy Guidelines and Principals

3.1 Scope

This policy applies to all Town officials, employees and contractors (hereinafter referred to as 'Users') whose access to or use of information and/or records and information technology resources that is provided by the Town or available through equipment owned by the Town whether or not that access is during normal working hours and whether such access is from the Town's premises or elsewhere.

3.2 Responsibilities

3.2.1 The Chief Administrative Officer (the 'CAO'), pursuant to FOIP Bylaw No. 684, is the FOIP Head for the Town, and some powers under FOIP have been delegated to the FOIP Coordinator for the Town.

3.2.2 The FOIP Coordinator is responsible for:

- a) ensuring that proper procedures are followed regarding information requests;
- b) responding to FOIP requests;
- c) recording and providing FOIP request statistics as required; and
- d) liaising with the Office of the Information and Privacy Commissioner on privacy breaches, privacy complaints and access appeals;

3.2.3 The Town will define privacy standards for information control and security systems and department managers are expected to ensure that this is adhered to within their departments and consistent with this policy. These will include:

- a) written privacy strategies, goals, procedures, standards and guidelines for the collection, use and disclosure of personal information;
- b) ensuring that managers, supervisors and employees receive appropriate privacy training, thereby providing adequate information to all employees with respect to their responsibilities under this policy;
- c) being responsible and accountable for personal information control and security systems in their departments; and
- d) ensuring that project teams include a Privacy Impact Assessment ('PIA') in the initial plan stage for the project or program and that resources are assigned to complete the PIA in the initial plan for the project.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|--|-----------------------|--------------|-------------|
| Title | Protection of Information and Privacy | | | Page 4 of 5 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

- 3.2.4 Employees are expected to respect the confidentiality of personal information and comply with the Town’s information control and security systems.
- 3.2.5 Employees will report any suspected or actual breaches of privacy to their immediate supervisor or other Town designated authority.
- 3.2.6 Section 82 of the FOIP Act permits an employee to disclose to the Information and Privacy Commissioner any information that the employee is required to keep confidential so long as the employee believes that the information should be disclosed, or if the information is being collected, used or disclosed in contravention of the privacy provisions of the FOIP Act or this policy.

3.3 Privacy Code

- 3.3.1 The Town recognizes that the privacy and confidentiality of the personal information of all persons is important and pledges to treat the personal information of all persons with respect and according to the Freedom of Information and Protection of Privacy (FOIP) Act and Regulations.
- 3.3.2 Employees are expected to familiarize themselves with and abide by the Town’s Privacy Code.

4.0 Privacy Impact Assessment

- 4.1 The Privacy Impact Assessment (‘PIA’) process was developed by the Office of the Information and Privacy Commissioner to assist public bodies in reviewing the impact that new projects may have on an individual’s privacy. Privacy consideration should be integrated at the earliest stages of the development of new programs, schemes or automated information systems to ensure that these reflect the requirements of FOIP.
- 4.2 This process is also designed to be used by the Town to evaluate existing programs or schemes to ensure compliance with FOIP.
- 4.3 Departments conducting a PIA will use the instructions and questionnaire from the Office of the Information and Privacy Commissioner, and will include:
 - a) a description of the project/program and of the nature and sensitivity of the personal information involved;



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|--|-----------------------|--------------|-------------|
| Title | Protection of Information and Privacy | | | Page 5 of 5 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

- b) a discussion of the relevant privacy principles and potential issues for the project, as well as suggestions as to how they should be addressed;
- c) a data flow analysis, including a description of the uses of the personal information and all consistent purposes and authorized disclosures;
- d) consideration of how the privacy requirements of FOIP will be met; and
- e) an overall assessment of the privacy impact (high, medium or low) and an analysis of threats and risks.

4.4 The CAO or designate will assist departments with the preparation of PIA's.

4.5 The CAO will consider and prioritize, within the context of the current annual work plan of the Administration Department, any written request from other Town departments to conduct the 'audit' portion of the Privacy Impact Assessment.

5.0 Compliance

5.1 Employees must report suspected violations or fraudulent activities pertaining to municipal records to their immediate supervisor and/or department manager.

5.2 Suspected violations that involve criminal conduct must be reported immediately to the Chief Administrative Officer or designate.

5.3 Any violation of this policy may subject the employee to their loss of access to records and use of communication and technology resources, and may result in disciplinary actions being taken, up to and including dismissal from employment.

5.4 Illegal acts involving communication and technology resources may also subject the user to restitution, commencement of civil action, or criminal investigation and prosecution by police agencies and/or local, provincial and federal authorities.



TOWN OF GRANDE CACHE
Policy and Procedures

Title **Protection of Mobile Devices and Mobile Data Storage Devices** Page 1 of 4

Section FOIP/IT Security **Resolution No.** 304/16
Department All **Effective Date** June 8, 2016

P
O
L
I
C
Y

Background

The Town of Grande Cache is committed to safe and responsible use of communication and technology resources to protect information collected and utilized in the daily operations of the Town. This policy protects the interests of the Town, users of the Town’s communication and technology resources and the public by providing a standard for the use, storage and protection of information held in the custody of the municipality.

1.0 Purpose

The purpose of this policy is to ensure the Town of Grande Cache employs consistent physical, administrative and technical access controls to safeguard employees and the public, and to protect the security of information and information technology resources, including mobile devices and mobile data storage devices.

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Employee means any individual employed by the Town, along with those individuals employed under contract by the Town.

Data is a general term used to denote any or all facts, numbers, letters and symbols that refer to or describe an object, idea, condition, situation or other factors in a computerized form.

Disclosure means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give personal information by any means to someone. This includes electronic transmission through electronic mail or data transfer.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Protection of Mobile Devices and Mobile Data Storage Devices | Page 2 of 4 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

Encryption Solution means Town-approved technical solutions for converting information into unreadable forms (via industry standard methods) which are essentially impossible to translate back into readable form without using the correct original encryption key.

FOIP Act means the Alberta Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 as amended.

Information means any information that identifies an individual or business and is stored in any format that the Town utilizes in the usual business operations of the municipality.

IT Resource means any Town-owned or controlled asset used to generate, process, transmit, store or access Town information.

Mobile Data Storage refers to any means of storing electronic information that is small and relatively portable. This includes but is not limited to laptop computers, tablets, notebooks, personal digital assistants (PDA's), smart phones, USB flash memory sticks, portable disk drives, diskettes, data tapes, CD's and DVD's.

Mobile Sensitive Data means sensitive data that is copied or moved off of Town Information Banks in any form. This is commonly copied onto mobile data storage, but may include many other situations (including from a server to a desktop computer or as an attachment sent by email).

Remote Access means a Town-approved method of electronically accessing data from Town Information Banks from outside of Town premises via remotely connecting and communicating with the Town system. This includes but is not limited to Outlook Web Access or other network solution approved by the Town.

Sensitive Data is a general term for electronic information not allowed to be released to any members of the public. Sensitive data includes but is not limited to personal information, business information related to a third party, draft documents or other information deemed to be confidential and exempted or excluded from release under the FOIP Act. This includes personnel information, credit or debit card, other financial or banking information and information classified as confidential.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|---|------------------------------------|
| Title | Protection of Mobile Devices and Mobile Data Storage Devices | Page 3 of 4 |
| Section | FOIP/IT Security | Resolution No. 304/16 |
| Department | All | Effective Date June 8, 2016 |

Town Information Banks refers to all forms of electronic information stored on Town servers, including but not limited to the electronic mail system, application databases, private and shared file directories, document repositories.

3.0 Policy Guidelines and Principals

3.1 General

Protection from unauthorized disclosure or release of sensitive data located on mobile devices or mobile data storage devices is the responsibility of each employee. Wherever possible, employees should avoid the risks of creating mobile sensitive data by leaving the data on Town information banks.

3.2 Protecting Mobile Devices and Mobile Data Storage Devices

- 3.2.1 To reduce the risk of theft or loss of mobile devices and mobile data storage devices, employees must follow mandatory security guidelines at all times. Please refer to 'Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices'.
- 3.2.2 Prior to using any sensitive data, employees must determine the level of risk ~ what is the impact to the Town if this data were to undergo inadvertent disclosure to unauthorized parties? Depending on the level of risk, additional protections may need to be followed where appropriate. Please refer to 'Guidelines for the Protection of Mobile Devices and Mobile Data Storage Devices'.
- 3.2.3 Managers are responsible for assisting employees in the assessment of risk and may need to contact the FOIP Coordinator or Chief Administrative Officer for direction.
- 3.2.4 Employees must consult with their supervisor in advance if they intend to take or copy sensitive data from the Town information banks.
- 3.2.5 All mobile sensitive data is to be considered a temporary copy and employees must delete it in a timely manner.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | | |
|-------------------|---|-----------------------|--------------|-------------|
| Title | Protection of Mobile Devices and Mobile Data Storage Devices | | | Page 4 of 4 |
| Section | FOIP/IT Security | Resolution No. | 304/16 | |
| Department | All | Effective Date | June 8, 2016 | |

3.3 Reporting Loss of Mobile Data Storage

Employees must report all lost or stolen mobile data storage immediately to the IT Resource Officer, along with a list of sensitive data contents. If personal information was present on the lost or stolen mobile data storage, a Privacy Breach report must be completed and submitted for immediate action.

3.4 Termination of Employment, Agreement, Contract or Appointment

3.4.1 Supervisors or managers shall contact the IT resource officer to remove the individual's electronic access privileges. The IT resource officer shall ensure all electronic access privileges, including disabling email accounts, are revoked upon termination of an individual's employment, contract, service or appointment with the Town.

3.4.2 All Town-owned equipment and devices must be immediately returned to the immediate supervisor, department manager or designated security officer.

4.0 Compliance

4.1 The Town's IT resources must be used in activities in compliance with all applicable laws or regulations, including without limitation, those:

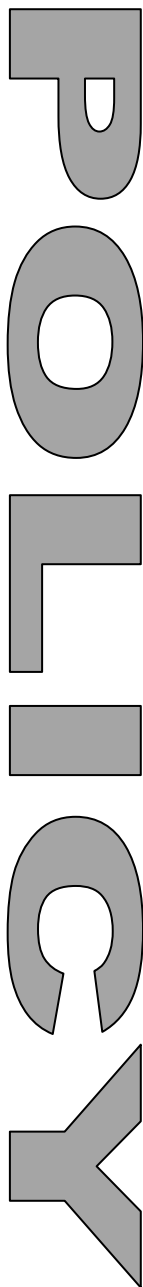
- a) at the federal, provincial and municipal level;
- b) those by way of international treaties;
- c) those of any foreign jurisdiction with authority;
- d) those civil laws in force between vendor and purchaser of IT resources; and
- e) any and all Town policies.

4.2 The Town's IT resources are to be used in a manner consistent with the Alberta Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25 and related Town policies.



TOWN OF GRANDE CACHE Policy and Procedures

| | | | |
|-------------------|--|-----------------------|----------------|
| Title | Records and Information Management and Security for Council | | Page 1 of 3 |
| Section | FOIP/IT Security | Resolution No. | 155/16 |
| Department | Council | Effective Date | April 13, 2016 |



1.0 Purpose

The purpose of this policy is to:

- a) formalize and clarify practices that apply to Council members in regards to records and information and the use and management of data created or received in the normal course of conducting Town business;
- b) ensure the consistent management of Council member’s paper and electronic records through the record’s life cycle;
- c) provide direction to Town Administration on the management of Council member’s paper and electronic records when that Councillor leaves office; and
- d) assist Council members to comply with the requirements of the Alberta Freedom of Information and Protection of Privacy Act.

2.0 Policy Statement

The Town of Grande Cache recognizes the importance of its Council members, in the performance of their duties, to be able to access information and communicate with each other, Town staff and other stakeholders in a timely and efficient manner. Records and information in the possession of Council members are assets that require management to ensure they serve both current operational purposes and potential legal and historical purposes.

3.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Council Members means elected officials of the Town.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | |
|-------------------|--|--------------------------------------|
| Title | Records and Information Management and Security for Council | Page 2 of 3 |
| Section | FOIP/IT Security | Resolution No. 155/16 |
| Department | Council | Effective Date April 13, 2016 |

Record means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers, and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records (*s. 1 (q) of the Alberta Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended*);

Records and Information Management is the application of systematic control over records throughout their life cycle, including but not limited to, forms management, manuals management, records inventory, file systems development and implementation, file maintenance procedures development, file equipment selection, correspondence and reports maintenance and records scheduling and disposition.

4.0 Policy Guidelines and Principals

4.1 Storage of Records and Information

Council members will operate in a manner which establishes and preserves records storage facilities for their records. The Town of Grande Cache allocates file storage space for Council members during their term of office.

It is recognized that some records are stored on the Town's computer server and it is the responsibility of the Chief Administrative Officer to ensure the integrity of the control and custody of the Council member who owns the records is preserved to the greatest extent possible through the use of data encryption, passwords and/or other techniques.

4.2 Handling of Records

Both the control and right of possession of a record remains with the Council member who owns the record.

4.3 Classification of and Retention Schedules for Council Member Records

Council members, at their sole discretion, may set classification categories for their records and corresponding retention schedules.



TOWN OF GRANDE CACHE
Policy and Procedures

| | | | |
|-------------------|--|-----------------------|----------------|
| Title | Records and Information Management and Security for Council | | Page 3 of 3 |
| Section | FOIP/IT Security | Resolution No. | 155/16 |
| Department | Council | Effective Date | April 13, 2016 |

To assist Council members in the handling of their records, Administration will recommend classification retention schedules for Council member’s records as a guide. These guidelines will be based on and similar to the classification system and retention schedules used by the Town for similar records in order to facilitate discussion of and exchange of records between Council and Administration.

4.4 Final Disposition of Council Member Records

When a Council member no longer requires a record or at the end of that Council member’s term of office, the final disposition of the records is at the sole discretion of the Council member. The Council member may direct that the records be destroyed, by shredding or recycling.

References

Council Code of Conduct Policy, Section C-1: Council, Town of Grande Cache Policy and Procedures Manual

Council Acceptable Use of Communication/Technology Resources, Section F-1: FOIP and IT Security, Town of Grande Cache Policy and Procedures Manual

| | | | |
|--|------------------------------------|--------------------------------------|--------|
| POLICY AND PROCEDURE MANUAL | Subject Training and Exercises | Section No. X-1 | Page 9 |
| | Department Emergency Management | Approved by Resolution No. 032/13 | |
| | Effective Date January 23, 2013 | Supersedes | |

TRAINING AND EXERCISES POLICY

Background

Emergency management response operations are generally divided into three main areas:

1. The actual emergency first response activities—usually operating at the emergency site.
2. The site coordination function, also referred to as site management.
3. The municipal coordination function, also called EOC operations.

All three functions are distinct, carried out by different agencies and personnel and require different training and equipment.

In this policy, the coordination functions of the EOC and site management are addressed. First responders typically have their own policies, a well-established training, exercises and equipment regimen within their respective agencies.

Training is required to perform in an effective and efficient manner in the EOC or site management. Training and planning are validated through exercises.

Risk

The municipal EOC and site management functions are carried out to ensure efficient and effective emergency management in a very specialized environment, often under stress and time pressure. To perform well in these circumstances, specialized training should be made available to, and required of all personnel that may work in these functions. Training is available from educational institutions, consultants, provincial government programs, federal government courses, on-line resources and many other sources.

A municipal training program needs to outline municipal emergency management functions, list all training resources, identify training requirements for each function, identify contingencies in each function, provide a training schedule for the next period (usually one year) and list all previous training and document follow-up. Once training is completed, regular exercises will validate planning procedures and that the training program is effective.

Recommended Policy

To ensure all functions outlined in the Town of Grande Cache Municipal Emergency Plan are carried out in an effective and efficient manner, a training and exercise plan shall be included in the Municipal Emergency Plan. This plan shall include a list of all personnel carrying out Emergency Management functions including contingencies, identify training requirements for each function and list training opportunities for each in yearly cycles.

| | | | |
|--|------------------------------------|--------------------------------------|---------|
| POLICY AND PROCEDURE MANUAL | Subject Training and Exercises | Section No. X-1 | Page 10 |
| | Department Emergency Management | Approved by Resolution No. 032/13 | |
| | Effective Date January 23, 2013 | Supersedes | |

Exercises shall be scheduled regularly in such a way that training and procedures will be verified through appropriate exercise objectives and formats. The DEM shall provide regular training and exercise reports to Council.

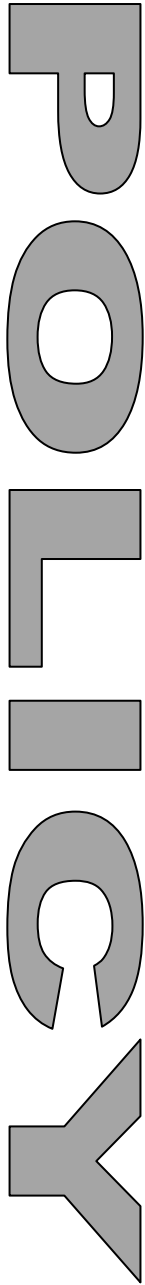


TOWN OF GRANDE CACHE Policy and Procedures

Title **Use of Surveillance Cameras**

Page 1 of 3

| | | | |
|-------------------|----------------------|-----------------------|------------------|
| Section | 5 – FOIP/IT Security | Resolution No. | 399/18 |
| Department | All | Effective Date | October 24, 2018 |



Background

The Town of Grande Cache (the Town) will utilize surveillance equipment, including cameras, for the purpose of protecting the Town’s equipment and resources from theft and vandalism and other unlawful acts, for the purpose of conducting an investigation into such matters. The collection, use, and disclosure of personal information shall comply with the *Freedom of Information and Protection of Privacy Act* and this Policy.

1.0 Purpose

The purpose of this policy is to establish guidelines for the use of surveillance to protect the Town’s assets and the collection, use, and disclosure of personal information.

2.0 Definitions

Town means the municipal corporation of the Town of Grande Cache.

Authorized Person means the individual employee or contractor of the Town who has been designated by the Chief Administrative Officer to access recordings created by Surveillance Technology and who has executed a non-disclosure agreement in form authorized by the Chief Administrative Officer.

Surveillance Technology means surveillance camera, microphones, or other equipment used for the purpose of monitor activities in a specific location.

Unlawful Activity means a violation of a federal, provincial or municipal law, regulation or bylaw, or the wrongful taking, destruction, vandalism, or defacing of any real of person property.



TOWN OF GRANDE CACHE
Policy and Procedures

Title Use of Surveillance Cameras

Page 2 of 3

| | | | |
|-------------------|----------------------|-----------------------|------------------|
| Section | 5 – FOIP/IT Security | Resolution No. | 399/18 |
| Department | All | Effective Date | October 24, 2018 |

Personal Information has the meaning given to it by the *Freedom of Information and Protection of Privacy Act* (Alberta) as amended from time to time

3.0 Policy

3.1 Principles

3.1.1 The Town may employ Surveillance Technology in order to:

- a) Discourage Unlawful Activity in relation to the Town’s assets; and
- b) Assist with investigations and prosecution of Unlawful Activity

3.1.2 Surveillance Technology shall be used in locations that:

- a) Have been or may be subject to Unlawful Activity; and
- b) Have been approved by the Chief Administrative Officer.

3.1.3 Surveillance Technology must be directed to focus on the approved locations, and must avoid areas where individuals could be recorded that would not be consistent with the purpose for which the Surveillance Technology was installed.

3.2 Notice

3.2.1 Prior to the use of Surveillance Technology at an approved locations, a notice shall be posted at all entry points indication the presence of Surveillance Technology and that Personal Information may be recorded.

3.2.2 The notice shall:

- a) Be in a form approved by the Chief Administrative Officer;
- b) Reference the *Freedom of Information and Protection of Privacy Act*; and provide the number and title of the Town’s employee who may answer questions about the Surveillance Technology.



TOWN OF GRANDE CACHE
Policy and Procedures

Title **Use of Surveillance Cameras**

Page 3 of 3

| | | | |
|-------------------|----------------------|-----------------------|------------------|
| Section | 5 – FOIP/IT Security | Resolution No. | 399/18 |
| Department | All | Effective Date | October 24, 2018 |

3.3 Recordings

3.3.1 Recordings created as a result of the use of Surveillance Technology shall be:

- a) Stored securely;
- b) Accessed by Authorized Personnel only;
- c) Used only for the purpose set out in this Policy;
- d) Destroyed 30 days following their creation, unless such recordings are required to be used or retained for a purpose set out in this Policy, or as otherwise required by law.