

Title:	Right of Access and Correction of Personal Information		
Policy No:	1048		
Effective Date:	June 9, 2026		
Motion Number:	26.181		
Responsible Department:	Legislative & Administrative Services		
Review Date:	June 9, 2029		
Legal References:		Cross References:	
Municipal Government Act, R.S.A., 1048, c.M-26. Protection of Privacy Act, S.A., 2024, c.P-28.5. Protection of Privacy AB. MReg., 132/2025. Access to Information, S.A., 2024, c.A-1.4. Access to Information AB. MReg., 133/2025.		Bylaw 22-929 Records Retention and Disposition Greenvview Schedule of Fees Policy 1042 Access to Information Policy 1047 Privacy Management Program	
Purpose:	The purpose of this policy is to establish a clear and consistent process for the administration of requests for access to information and for the correction of personal information held by Greenvview. This policy supports the timely, accurate, and consistent handling of requests in accordance with applicable legislation, while ensuring that personal information is managed responsibly and in a manner that respects privacy and confidentiality.		

1. DEFINITIONS

- 1.1. **Acts** means the Access to Information Act, S.A., 2024, c.A-1.4 and the Protection of Privacy Act, S.A., 2024, c.P-28.5.
- 1.2. **Applicant** means the person who makes a request for access to records under the Access to Information Act.
- 1.3. **CAO** means the Chief Administrative Officer, or their designate.
- 1.4. **Custody or Control** means custody is the effective physical possession of information; control is responsibility and accountability for making decisions about the handling of information, regardless of whether Greenview has custody of the information Greenview has control over any information that any of its officials, employees, or service providers has created or received as part of their mandated functions and activities, regardless of the location of the information or the time of collection, use, or disclosure.

- 1.5. **Data Derived from Personal Information** means data created or derived from data matching that identifies individuals whose personal information was used in the data matching process. May include AI Inferences.
- 1.6. **Disclosure** means giving access to or making the personal information in Greenview's custody or control available to a person or organization external to Greenview.
- 1.7. **Employee** means the persons employed by Greenview, in any capacity.
- 1.8. **Greenview** means the Municipal District of Greenview No. 16.
- 1.9. **Individual** means any person, living or deceased, regardless of residency, citizenship, or status. In addition, the authorized representative of the individual.
- 1.10. **Non-personal Data** means data, including data derived from personal information and synthetic data, that has been generated modified or anonymized so that it does not identify any individual.
- 1.11. **Personal Information** means information about an identifiable individual, including the individual's name; home address, telephone number, email address, or other personal contact information; race, national or ethnic origin, colour, or religious or political beliefs, or associations; age, sex, marital or family status; identifying numbers or other unique identifiers; fingerprints, blood type, or other biological information; educational, financial, employment, or criminal history; the individual's personal views or opinions; and the views or opinions of another individual about that individual, but does not include contact information of an individual acting in a business professional, or official capacity where it is provided on behalf of an employer or organization.
- a) Name
 - b) Address, telephone, email, or contact information*
 - c) Race
 - d) National or ethnic origin
 - e) Colour
 - f) Religion
 - g) Political beliefs or associations
 - h) Age
 - i) Sex
 - j) Marital status
 - k) Family status
 - l) Identifying numbers
 - m) Fingerprints or blood type
 - n) Educational, financial, employment, criminal records

- o) Opinions about the individual
- p) Individual's personal views or opinions (except opinions about others)
- q) Home or business address, telephone, email or other contact information of an employee of a public body, or any individual is not personal information, if it is provided on behalf of the employer in the individual's capacity as employee or agent.

Personal information under ATIA and POPIA that is not normally excepted from disclosure:

- a) Opinions contained in work product;
- b) Classification, salary range, discretionary benefits, or employment responsibilities of public body employees;
- c) Financial and other details of a contract to supply goods or services to a public body;
- d) Information about a license, permit, financial or other discretionary benefit granted to an individual by a public body;
- e) Information is about an individual who has been dead for 25 years or more; and,
- f) Information is about an individual's enrolment at a school, attendance at a public event, or receipt of an award granted by a public body.

1.12. **Record** means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio, or other medium, but does not include any software or other mechanism used to store or produce the record.

1.13. **Significant Harm** means harm that results from the unauthorized access, disclosure, or loss of personal information, including:

- a) Bodily harm;
- b) Humiliation;
- c) Damage to reputation or relationships;
- d) Loss of employment or business or professional opportunities;
- e) Identify theft;
- f) Diminished insurability;
- g) Diminished credit;
- h) Loss of property or legal status; and,
- i) Loss of finances;

The following factors are also considered in determining the significance of harm:

- j) It is reasonably believed that the information has been or will be misused;

- k) The unauthorized access, disclosure of loss was the result of malicious intent;
- l) The personal information is sensitive; and,
- m) Existing mitigating factors reduce the risk of significant harm

1.14. **Third Party** means a person, a group of persons or an organization other than the applicant making an access request, or other than the employees and officials of Greenview.

2. POLICY STATEMENT

- 2.1. This policy governs all Greenview employees including directors, officers, contractors, students, and volunteers providing services on behalf of Greenview.
- 2.2. This policy applies to all recorded information, in any form or medium, including paper, digital, audio-visual, and graphic records, created or received in the course of carrying out Greenview's mandated functions and activities.
- 2.3. All facilities, systems, and equipment used to collect, create, access, store, process, transmit, or otherwise manage Greenview information are subject to this policy.

3. RECEIVING AND FACILITATING REQUESTS

- 3.1. Requests for access to Greenview information can be made by any individual or organization (the applicant), regardless of location or status. A public body may not make a request to another public body.
- 3.2. Greenview responds to right of access requests openly, accurately and completely and will:
 - a) Engage with applicants to allow them to clarify their request so it can be processed;
 - b) Respond to questions in plain language; and,
 - c) Assist applicants in adjusting requests so they can be processed.
- 3.3. Greenview does not deny access to information based on the applicant's reason or purpose for the request.
- 3.4. Requests for information under ATIA may contain personal information of the applicant, which will be protected and managed in accordance with POPA.
- 3.5. Requests for access to records that are not the applicant's own personal information may be subject to fees established by Greenview's Schedule of Fees Bylaw.
- 3.6. Once the applicant has met the requirements to make a request, Greenview has 30 business days to respond, unless the request has been abandoned, disregarded or transferred, or if the time limit is extended in accordance with ATIA.

4. EXCLUDED RECORDS

- 4.1. Some records that are in the custody or control of Greenview are excluded from the ATIA and do not have to be considered relevant or released as part of a right of access request.

However, Greenview may choose to release this information as part of a request under specified circumstances. Excluded records include:

- a) Records designated by Greenview as available without a request;
- b) Court and administrative support records created or received by the courts of Alberta, including justices of the peace;
- c) Records created or received by officers of the Alberta Legislature, including the Office of the Information and Privacy Commissioner, Ethics Commissioner, Auditor General, and the Public Interest Commissioner;
- d) Records and copies of records from a provincial or public body registry office, including the Personal Property Registry, Corporate Registry, Motor Vehicles Registry, Land Titles Office, and the Vital Statistics Registry;
- e) Greenview records that have already been made public by other means;
- f) Records in the custody or control of the federal, provincial or territorial government and their agencies;
- g) Personal or constituency records of an elected or appointed member of the governing body of Greenview;
- h) Health records created or received by a Greenview doctor or nurse; and
- i) A question used on an examination or test only if release does not jeopardize a standardized or continuing evaluative process.

4.2. Records received from private sector donors and preserved in Greenview archives for historical or research purposes are excluded from the application of this policy and shall only be used or disclosed with the consent of the individual or organization to whom the information relates.

4.3. Data derived from personal information and non-personal data cannot be released in response to a right of access request.

5. DISREGARDING REQUESTS

5.1. Greenview disregards a right of access request only in exceptional circumstances when:

- a) The information requested is already available to the applicant or to the public;
- b) After initial requests from Greenview for clarification, the applicant has not provided enough detail to make it comprehensible or to locate the requested information;
- c) The request has been made repeatedly, as part of a pattern of conduct that is systematic, regular and deliberate;
- d) The applicant makes use of abusive, threatening, or harassing language or actions during the application or facilitation process; or
- e) The request is abusive, threatening, frivolous or vexatious.

- 5.2. The applicant is informed of the reasons for disregarding the request and the right to ask the Commissioner to review Greenview's decision.

6. SEARCHES FOR RELEVANT RECORDS

- 6.1. Greenview makes every effort to identify and retrieve for review all records in its custody or control that are relevant to an applicant's request. This will include information in any location and format and on any devices, accounts and platforms not owned by Greenview, that was created or received by employees and contractors to support their functions as Greenview officials.
- 6.2. The search for records relevant to an applicant's request includes all electronic records that can be accessed or produced using normal computer hardware, software and technical expertise and would not unreasonably interfere with its operations. This includes:
- a) Reports or extracted data sets from existing databases that can be constructed and generated using existing software and expertise, but does not include the creation of information that is an analog summary, analysis, consolidation or digest of existing information that did not exist prior to the request; and
 - b) Emails, text messages, and social media posts sent or received on any account or platform that were created or received to support functions and activities of the public body.
- 6.3. Greenview's Records & Information Coordinator, responsible for responding to a request, is authorized to access and retrieve for review any personal or general information on any device or platform that is required to identify, retrieve records relevant to a request.

7. REVIEWING AND WITHHOLDING INFORMATION

- 7.1. Greenview only withholds information relevant to the request when it is determined that mandatory or discretionary or exceptions to the right of access apply to the records requested.
- 7.2. Greenview must refuse to disclose information in response to a right of access request if the release would be:
- a) harmful to business interests of a third-party business;
 - b) an unreasonable invasion of a third party's personal privacy; or
 - c) harmful to provincial Cabinet and Treasury Board confidences, as long as the information is in a record for less than 15 years or result in the release of a record that was submitted to or prepared for submission to the Executive Council, the Treasury Board or one of their committees, or was created on or on behalf of any of the above.
- 7.3. Greenview may refuse to disclose information in response to a right of access request if the disclosure could reasonably be expected to:

- a) Threaten anyone's safety or mental or physical health; interfere with public safety; or cause an applicant to do immediate and grave harm to themselves or others;
- b) Reveal confidential evaluations conducted pre-hire or pre-contract award;
- c) Harm a law enforcement matter;
- d) Harm a workplace investigation;
- e) Harm inter-governmental relations;
- f) Reveal local public body confidences, including drafts of bylaws, resolutions, legal instruments and the substance of deliberations of in-camera meetings;
- g) Reveal advice, proposals, recommendation, analyses or policy options developed by or for the public body;
- h) Cause harm to the economic interests of Greenview or the Alberta Government;
- i) Reveal information relating to testing or auditing procedures;
- j) Reveal legally privileged information;
- k) Cause harm to conservation of heritage sites; or
- l) Reveal information that is already or will be made available to the public within 60 business days.

8. PUBLIC HEALTH AND SAFETY OVERRIDE

8.1. Greenview discloses without delay, to the public, a group of people, an individual, or an applicant, any information that Greenview has about a risk of significant harm to the environment or to the health and safety of the public, a group of people, an individual or an applicant.

8.2. Before disclosing the information, Greenview must, where practicable, notify any third party to whom the information relates, give the third party an opportunity to make representations relating to the disclosure and notify the Commissioner.

9. THIRD PARTY REVIEWS

9.1. Where it is unclear whether the disclosure of records may adversely affect a third party, Greenview shall notify the affected third party and request their input where the records may contain information that could reasonably be expected to:

- a) Harm the business interests of a third party; or
- b) Constitute an unreasonable invasion of a third party's personal privacy.

10. REQUESTS FOR CORRECTION OR AMENDMENT OF PERSONAL INFORMATION

10.1. Individuals may request correction or amendment of their own personal information in the custody or control of Greenview.

10.2. Greenview will not amend professional opinions that are made by employees that have the competency to make them.

11. ADMINISTRATION RESPONSIBILITIES

- 11.1. The Records & Information Coordinator, as designated by the CAO, is responsible for Greenview's access to information and privacy obligations in accordance with applicable legislation and delegated authority.
- 11.2. Department Managers are responsible for implementing and maintaining privacy and security practices within their respective areas and ensuring compliance with this policy, and shall:
- a) Support employee awareness of, and training on, privacy and security policies and procedures;
 - b) Refer all formal access to information requests to the Records & Information Coordinator;
 - c) Assist in locating and retrieving records relevant to access requests; and
 - d) Ensure contracted third parties comply with applicable privacy and security requirements.
- 11.3. All employees and service providers are responsible for protecting and managing information in accordance with this policy, and shall:
- a) Cooperate in the processing of access requests and related compliance activities;
 - b) Access, use, disclose, and protect information in accordance with this policy and applicable legislation; and
 - c) Refer to the Records & Information Coordinator for any decisions regarding access or disclosure that are not clearly addressed by policy.