POLICY

Municipal District of GREENVIEW

Title:	Privacy Breach Response
Policy No:	1052
Effective Date:	August 25, 2026
Motion Number:	26.389
Responsible Department:	Legislative & Administrative Services
Review Date:	August 25, 2029

Legal References:	**Cross References:**
Municipal Government Act, R.S.A., 2000, c.M-26. Protection of Privacy Act, S.A., 2024, c.P-28.5. Access to Information Act, S.A., 2024, c.A-1.4.	Policy 1047 Privacy Management Program Policy 1031 Cyber Security Policy 1050 Privacy and Access Complaints

Purpose: The purpose of this policy is to ensure privacy breaches are promptly reported, managed, investigated, and resolved to minimize harm and support compliance with legislative requirements.

1. DEFINITIONS

1.1. **Administration** means the Chief Administrative Officer or any employee of Greenview who is accountable to the CAO.

1.2. **Greenview** means the Municipal District of Greenview No.16.

1.3. **Privacy Breach** means an unauthorized disclosure, use, destruction, loss, removal, or modification of information in the custody or control of Greenview. Events are considered unauthorized by reference to access, privacy and security policy and/or legislation. A breach may be accidental or the result of a deliberate act.

1.4. **Remedial Action** means steps taken to contain a breach, reduce harm, correct deficiencies, and prevent similar incidents from occurring in the future.

1.5. **Risk** means the likelihood and potential severity of harm resulting from a Privacy Breach, having regard to the nature and sensitivity of the information involved, the circumstances of the breach, and the individuals or organizations that may be affected.

1.6. **Security Classification** means the assigned level of sensitivity of information based on the potential harm that could result from unauthorized access, use, disclosure, modification, loss, or destruction.

2. POLICY STATEMENT

2.1. Ensure privacy breaches are assessed in a consistent and Risk-based manner.

2.2. Ensure appropriate action is taken to contain privacy breaches and mitigate potential harm.

2.3. Support fair, objective, and confidential investigations of privacy breaches.

2.4. Enable Greenview to respond to privacy breaches in a timely and effective manner.

2.5. Ensure compliance with applicable privacy legislation and regulatory requirements.

2.6. Promote continuous improvement of privacy safeguards and practices through the review of privacy breaches and corrective actions.

3. DETERMINING LEVEL OF RESPONSE

3.1. The severity of the breach determines the nature of the response reporting structure, remedial action, and the investigation process. In the response process, severity is based on:

3.1.1. The security classification of the information, which takes into account potential and real harm to individuals and organizations;

3.1.2. The internal and external scope and scale of the breach;

3.1.3. The known relationship of the recipients to subject individuals; or

3.1.4. The intentionality of the cause.

3.2. Levels are determined based on the designated classes and circumstances, including an assessment of the Risk of significant harm resulting from the breach.

3.3. Where a Risk of significant harm exists, Greenview will notify the:

3.3.1. impacted individuals

3.3.2. Office of the Information and Privacy Commissioner (OIPC), and;

3.3.3. Minister of Technology and Innovation

4. NOTIFICATION AND SUPPORT FOR IMPACTED INDIVIDUALS

4.1. Where a privacy breach poses a Risk of significant harm to an individual, Greenview will provide the individual with sufficient information to enable them to take reasonable steps to protect their personal information and mitigate potential harm.

4.2. Depending on the nature of the breach, impacted individuals are encouraged to:

4.2.1. Review the breach notification to understand the personal information involved and the potential Risks associated with the breach.

4.2.2. Monitor financial accounts, online accounts, and other relevant records for unauthorized activity or suspicious transactions.

4.2.3. Change passwords, security questions, and personal identification numbers (PINs) for affected accounts and enable multi-factor authentication where available.

4.2.4. Contact their financial institution if banking or payment information may have been compromised.

4.2.5. Obtain and review their credit report and consider requesting a fraud alert or credit monitoring service where appropriate.

4.2.6. Replace government-issued identification or other credentials if they have been compromised.

4.2.7. Exercise caution when responding to unsolicited emails, telephone calls, text messages, or other communications requesting personal or financial information.

4.2.8. Report suspected identity theft, fraud, or criminal activity to the appropriate law enforcement agency, financial institution, or the Canadian Anti-Fraud Centre, as applicable.

4.2.9. Contact Greenview for additional information regarding the breach or the measures being taken to mitigate its impact.

4.3. Where appropriate, Greenview may provide impacted individuals with additional resources or support, including information on available protective services, recommended mitigation measures, and contact information for relevant regulatory or law enforcement agencies.

4.4. Individuals who have concerns regarding Greenview's handling of their personal information or its response to a privacy breach may submit a privacy complaint in accordance with Policy 1050 Privacy and Access Complaints.

5. INVESTIGATION PRINCIPLES

5.1. Greenview uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of persons being investigated. Investigations will, as required, incorporate the following methodologies:

5.1.1. Keep investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;

5.1.2. Use surveillance or monitoring data to establish past or current actions on an as-needed basis;

5.1.3. Examine or confirm the veracity of facts or statements, sometimes using third party witnesses;

5.1.4. Inform participants of their status and the progress of the investigation as fully and quickly as possible so long as it does not jeopardize the integrity of the investigation;

5.1.5. Base findings and conclusions on balance of probabilities.

5.2. The breach investigation is an administrative rather than a disciplinary process. Once the report is delivered, it is the responsibility of Management and Human Resources to determine the appropriate disciplinary action.

6. COUNCIL RESPONSIBILITIES

6.1. Approve this policy and support Greenview's commitment to protecting personal information and complying with applicable privacy legislation.

7. ADMINISTRATION RESPONSIBILITIES

7.1. Protect information in its custody or control through appropriate administrative, technical, and physical safeguards.

7.2. Maintain processes to identify, report, assess, contain, investigate, and respond to privacy breaches.

7.3. Assess privacy breaches to determine the Risk of harm and the need for notification or further action.

7.4. Notify affected individuals and regulatory authorities, when required by applicable legislation.

7.5. Take reasonable steps to mitigate harm resulting from a privacy breach and to prevent similar incidents from occurring in the future.

7.6. Review and improve privacy practices, procedures, and safeguards on an ongoing basis.