RESOLUTION NO: 2025-07

PRIVACY POLICY

WHEREAS the City Council of Lake Point is entrusted with legislative and oversight responsibilities to serve the public interest while safeguarding the privacy and dignity of its employees and citizens;

WHEREAS the Utah Government Records Access and Management Act (GRAMA) [Utah Code § 63G-2-302] provides explicit protections for private records, to prevent unnecessary disclosure and potential misuse;

WHEREAS access to sensitive records by City Council members and staff members without actual oversight for those records, including government officials, whether they were elected or appointed, will prevent privacy concerns among employees and community members;

WHEREAS repeated access to and misuse of detailed records by elected officials may undermine ethical obligations as outlined in Utah Code as currently amended, which prohibits the use of public office for improper influence or special privileges;

WHEREAS this policy consolidates privacy practices, outlines governance roles and responsibilities, and ensures compliance with generally applicable records management, data protection, and data privacy obligations. It is designed to safeguard individual privacy rights, promote transparency, maintain the integrity and security of personal data, and ensure accountability across Lake Point. This policy is meant to guide further alignment of Lake Point with the State Data Privacy Policy.

NOW, THEREFORE, BE IT RESOLVED by the City Council of Lake Point, that the following policies and practices are hereby adopted to protect the privacy of employees and citizens while ensuring the Council can fulfill its oversight duties:

Section 1. Purpose

1. This policy applies to Lake Point's privacy program, which includes policies, practices, and procedures for protecting the privacy of employees and the processing of personal data in accordance with Utah Code as currently amended, and which aligns with the records management and data governance requirements provided in both GRAMA and DARS. Where applicable, this policy will refer to a more specific or detailed policy, procedure, or guidance that addresses a particular practice that Lake Point has developed.

Section 2. Scope

1. This policy applies to all Lake Point employees involved in the management, creation, and maintenance of records or who have access to personal data as part of their job duties. This policy also applies to all contractors of Lake Point that process or have access to personal data as a part of the contractor's duties under an agreement with Lake Point. This policy also applies to any elected or appointed officials who have access to personal data as part of their duties.

Section 3. Definitions

1. "Classification," "classify," and their derivative forms mean determining whether a record series, record, or information within a record is public, private, controlled, protected, or exempt from disclosure under Utah Code as currently amended.
2. "Cookie" means "Technology that records a user's information and activity when the user accesses websites. Cookies are used by website owners, third parties, and sometimes threat actors to gather user data."
3. "Data breach" means— the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised."
4. "Individual" means a human being.
5. "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.
6. "Personally identifiable information" means information that identifies:
    a. a user by:
        i. name;
        ii. account number;
        iii. physical address;
        iv. email address;
        v. telephone number;
        vi. Social Security number;
        vii. credit card information; or
        viii. bank account information;
7. "Processing activity" means any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.
8. "Record" means the same as that term is defined at Utah Code § 63G-2-103(25).
9. "Record series" means a group of records that may be treated as a unit for purposes of designation, description, management, or disposition.
10. "Records officer" means the individual appointed by the chief administrative officer of each governmental entity, or the political subdivision to work with state archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records.
11. "Schedule," "scheduling," and their derivative forms mean the process of specifying the length of time each record series should be retained by a governmental entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to the state archives or destroyed.

Section 4. Chief Administrative Officers (CAO)

1. The Chief Administrative Officer for Lake Point is the City Council Chair.

a. The designation of the CAO shall be reported to the Utah Division of Archives and Records Services (Archives) within 30 days of the designation.
    i. The designation of the City Council Chair as Chief Administrative Officer (CAO) is strictly for the purpose of state records compliance and does not grant additional supervisory authority beyond that held by other Council members. All decisions regarding sensitive data access must be approved by a majority vote of the Council or Utah law.
b. Designation of Duties
    i. The CAO is responsible for approving policy alignment with state privacy requirements, ensuring designation of records officers, overseeing completion of required trainings, and reporting data-sharing and breach response activities as required by law.
    ii. The Chief Administrative Officer (CAO), designated as the City Council Chair for purposes of compliance with state records management and data privacy laws, holds no supervisory authority beyond that of other Council members. The designation is strictly administrative and shall not be construed to grant unilateral decision-making authority or expanded access to sensitive records. The duties of the CAO, as relevant to this policy, shall include:
        1. Reporting the designation of the CAO to the Utah Division of Archives and Records Services (Archives) within 30 days.
        2. Ensuring municipal compliance with records creation, classification, retention, and disposal as required by DARS and GRAMA.
        3. Overseeing completion of Privacy Impact Assessments (PIAs) for IT systems processing personal data, as required.
        4. Coordinating with the City Recorder (ARO), City Attorney, and designated staff to uphold data protection standards.
        5. Ensuring required privacy training and certification for staff and officers occurs in a timely manner.
    iii. Any policy decisions or approvals requiring interpretation or application of privacy standards may be reviewed and revised by vote of the City Council to preserve equal legislative authority.

Section 5. Appointed Records Officers (AROs)

1. The City Recorder is the designated ARO and shall serve as records officer in fulfilling the duties of working with Archives and the Office of Data Privacy in the care, maintenance, scheduling, disposal, classification, designation, access, privacy, and preservation of records.
    a. A designated CAO may assign responsibility for the duties of appointed records officers to one, or among several, officers as the CAO deems appropriate.
    b. The appointment of records officers shall be reported to Archives within 30 days of the appointment.

Section 6. Privacy Officer

1. The Privacy Officer shall be appointed by the City Council to oversee the implementation, monitoring, and refinement of privacy practices within Lake Point. This role may be fulfilled by an existing officer or staff member with appropriate qualifications, or assigned externally by contract.
2. The duties of the Privacy Officer shall include:
    a. Ensuring compliance with all applicable data privacy laws, including GRAMA, DARS, and Utah Code § 63A-19-401 et seq.
    b. Assisting departments and contractors in the completion and documentation of Privacy Impact Assessments (PIAs).
    c. Serving as a liaison to the Utah Office of Data Privacy and Security (ODPS) and providing annual reports to the Chief Privacy Officer.
    d. Supporting the City Recorder in maintaining accurate privacy annotations for record series.
    e. Providing consultation on data-sharing agreements, internal procedures, and investigations related to data breaches or misuse of records.
    f. Collaborating with the City Attorney and City Recorder to investigate any privacy-related complaints submitted to the city.
    g. The Privacy Officer shall act in an advisory and administrative capacity and shall not have unilateral authority to access or authorize access to sensitive records without adherence to the policies herein.

Section 7. Records and Records Series

1. Lake Point shall create and maintain records and record series in accordance with the requirements provided in DARS and GRAMA in addition to correlated guidance issued by Archives.
2. Lake Point shall appropriately designate and classify records and record series in accordance with the requirements provided in DARS and GRAMA.
3. CAO(s) shall be responsible for submitting a proposed retention schedule for each type of material defined as a record under GRAMA to the state archivist for review.

Section 8. Record Series Privacy Annotation

1. The ARO shall perform a privacy annotation for each record series that contains personal data pursuant to Utah Code § 63A-12-115.
2. Privacy annotations shall include:
    a. the legal authority under which personal data is processed;
    b. the purposes and uses for the personal data; and
    c. the types of personal data that may be processed within the record series.
3. Privacy annotations shall be conducted and reported in accordance with additional requirements provided by Archives via administrative rule.

Section 9. Awareness & Training

1. Departmental Data Privacy Training
    a. The CAO of Lake Point shall ensure that all employees that have access to personal data as part of the employee's work duties complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year.
    b. The CAO of Lake Point is responsible for monitoring the completion of data privacy training by employees.
2. Appointed Records Officer Training and Certification
    a. GRAMA Access AROs: AROs who handle GRAMA transparency responsibilities are required to complete the GRAMA transparency training and obtain certification from the Archives in accordance with Utah Code § 63A-12-110.
    b. Records Management and Privacy AROs: AROs specializing in records management or privacy are required to complete both records management and GRAMA transparency training, as well as obtain the corresponding certifications.
3. Information Technology Privacy Impact Assessment
    a. The CAO shall ensure that the division completes a Privacy Impact Assessment (PIA) for all IT systems that may process personal data prior to the initiation of data processing in the IT system as required.
    b. The responsible CAO shall use the PIA template that is created and maintained by the Chief Privacy Officer and which is approved by the Chief Information Officer.
    c. CAOs must maintain a copy of each completed assessment for a period of four years to provide audit documentation and ensure accountability in privacy practices.

Section 10. Transparency

1. Website Privacy Policy
    a. The CAO shall create and maintain privacy policies on their websites as outlined in Utah Code § 63D-2-103 and Utah Admin. Code R895-8.
    b. The CAO shall ensure that personal data related to a user of a Lake Point city's website is not collected unless the Lake Point city's website complies with Utah Code § 63D-2-103(2).
    c. The CAO shall ensure that all websites of Lake Point contain a privacy policy statement that discloses:
        i. The identity of the governmental website operator;
        ii. How the governmental website operator may be contacted;
        iii. The personal data collected by the governmental entity;
        iv. The practices related to the disclosure of personal data collected by the governmental entity and/or the governmental website operator; and
        v. The procedures, if any, by which a user of a governmental entity may request:
            1. Access to the user's personal data; and
            2. Access to correct the user's personal data.

vi. A general description of the security measures in place to protect a user's personal data from unintended disclosure.

2. Privacy Notice
    a. Employees shall only collect personal data from individuals if, on the day the personal data is collected, Lake Point has provided a privacy notice to an individual asked to furnish personal data that complies with Utah Code §§ 63G-2-601(2), 63A-19-402, 63D-2-103(2)-(3), or other governing law, as applicable.
    b. Such a personal data request privacy notice shall generally include:
        i. the record series that the personal data will be included in;
        ii. the reasons the person is asked to furnish the information;
        iii. the intended purposes and uses of the information;
        iv. the consequences for refusing to provide the information; and
        v. the classes of persons and entities that currently:
            1. share the information with Lake Point; or
            2. receive the information from Lake Point on a regular or contractual basis.
    c. Individual Requests
        i. The CAO shall ensure that Lake Point has established appropriate processes and procedures that facilitate compliance with applicable governing law for handling the following privacy requests of individuals:
            1. Individual's requests to access their personal data;
            2. Individual's requests to amend or correct their personal data;
            3. Individual's requests for an explanation of the purposes and uses of their personal data; and
                a. At-risk governmental employee requests to restrict access to their personal data.

Section 11. Processing

1. Minimum Data Necessary
    a. The CAO shall ensure that all programs within Lake Point obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose.
    b. The CAO shall ensure that all programs within Lake Point regularly review their data collection practices to ensure compliance with the data minimization requirement.

2. Record and Data Sharing or Selling Policy
    a. Lake Point will only share or disclose personal data when there is appropriate legal authority. The sale of personal data is prohibited unless required by law.
    b. Data sharing must comply with GRAMA or other governing law and may include sharing with governmental entities, contractors, private providers, or researchers. Compliance with GRAMA or other governing law is contingent upon the purpose of the sharing, the parties involved, and the nature of the records.

c. The CAO is required to report annually to the Chief Privacy Officer on personal data sharing and selling activities, including types of data shared, the legal basis for sharing, and the entities receiving this data.

d. All contracts involving personal data must incorporate appropriate privacy protection terms. Written agreements for data sharing are recommended to ensure compliance with applicable laws and regulations.

3. Retention and Disposition of Records Containing Personal Data
    a. Employees shall maintain, archive, and dispose of records—which includes all personal data—in accordance with an approved retention schedule.
    b. Employees shall comply with all other applicable laws or regulations related to retention or disposition

Section 12. Information Security

1. Incident Response

a. Lake Point will adopt and follow the DTS Cybersecurity Incident Response Plan to manage and address all security incidents, including data breaches, and privacy violations.

b. Employees shall report all suspected security incidents, including non-IT incidents such as unauthorized access to physical records, to the Enterprise Information Security Office (EISO). Any additional agency-specific response measures for non-IT incidents are the responsibility of the CAO to develop and implement as appropriate.

c. The CAO shall ensure compliance with all other applicable laws or regulations related to incident response and breach notification of specific personal data held by Lake Point.

2. Breach Notification
    a. Lake Point is required to provide notice to an individual or the legal guardian of an individual, if the individual's personal data is affected by a data breach in accordance with Utah Code § 63A-19-406.
    b. Lake Point is required to notify the Cyber Center and the state attorney general's office of a data breach affecting 500 or more individuals in accordance with Utah Code § 63A-19-405. [Divisions] that experience a data breach affecting fewer than 500 individuals must create and report an internal incident report in accordance with Utah Code § 63A-19-405(5). These requirements are in addition to any other reporting requirement that the [division] may be subject to.

Section 13. Surveillance

1. Covert Surveillance
    a. A governmental entity may not establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law.
    b. The CAO shall ensure that surveillance activities are documented and that a PIA for the activity has been completed.

Section 14. Cookies, Fingerprinting, Key Loggers, and Tracking Technologies

1. Lake Point is committed to transparency and privacy protection for individuals that visit a website of the Lake Point with regard to the use of any tracking technologies, including but

not limited to cookies, device fingerprinting, key loggers, and other similar methods for monitoring or collecting information from website users.

a. Cookies
    i. The use of cookies on Lake Point's websites and digital services must comply with applicable privacy and security policies. Cookies should be limited to essential operational purposes, and any use of tracking or third-party cookies for analytics or similar functions must be disclosed clearly to users, with an option to consent where required by law.
b. Device Fingerprinting
    i. Device fingerprinting is prohibited unless explicitly authorized by the Council majority and where the legal basis or appropriate justification for such processing is documented in a privacy impact assessment. The purpose and extent of fingerprinting must be clearly defined, documented, and disclosed to users in a privacy notice or statement that complies with applicable legal requirements.
c. Other Tracking Technologies
    i. The use of other tracking technologies, such as web beacons, pixel tags, keyloggers, or similar tools, is prohibited unless explicitly authorized by the Council majority, and the legal basis for such tracking is documented in a PIA. Disclosure of these technologies must be included in user-facing privacy statements, with user consent obtained when required by law.
d. User Notification and Consent
    i. Lake Point must ensure users are informed about the use of tracking technologies. A clear website privacy statement must explain the types of data collected, the purpose of the tracking, and how users can manage their preferences or consent. Any updates to tracking practices must be promptly reflected in the privacy statement.
e. Data Security and Retention
    i. Data collected through authorized tracking technologies must be securely stored, with access limited to authorized personnel. Retention of this data must align with approved retention schedules, and the data should only be retained as long as necessary for the defined operational purpose.

Section 15. Internal Records

1. Designation of Sensitive Records
    a. A note prepared by the originator for the originator's own use or for the sole use of an individual for whom the originator is working is not classified as a record under GRAMA.
    b. Citizen account records may include private elements (such as contact information, account numbers, or billing history) subject to redaction under Utah Code § 63G-2-302. These records will be handled in accordance with their GRAMA classification and redacted where required.

c. Aggregated or anonymized summaries of the above records will be prepared for Council review to ensure oversight needs are met without revealing unnecessary personal details.

2. Role-Based Access Controls
    a. Only designated administrative staff with direct responsibilities for managing employee timecards or citizen accounts shall have access to detailed records.
    b. Elected/appointed officials, including City Council members, shall have access to summary reports and high-level data sufficient to perform their oversight responsibilities. Detailed records shall not be accessible without documented justification and the consensus of the city attorney
    c. . If approved, access must be restricted to the minimum necessary information required to address the specific concern.
    d. The City Attorney will determine the minimum necessary information required to address the specific concern.
    e. No individual Council member may compel, pressure, or otherwise influence staff to provide access to individual citizen or employee records outside the scope of this policy.

Section 16. Reporting Concerns Regarding Misuse of Sensitive Records or Data Privacy Complaints

1. Any citizen, or employee, contractor, appointed officer/member of the city can submit a privacy complaint to the Utah State Privacy Ombudsperson on the Utah Office of Data Privacy website and/or email the City Recorder directly or the Chief Administrative Officer of the City.
2. Investigation Procedure if complaint is submitted to the city:
    a. The City Recorder shall acknowledge receipt of the complaint within five business days.
    b. The City Recorder, in collaboration with the City Attorney, shall conduct a thorough investigation to determine the validity of the complaint.
    c. A final report, including findings and recommended actions, shall be submitted to the City Council within 30 days of receiving the complaint.
3. Anti-Retaliation/Whistleblower Protections:
    a. Retaliation against employees or citizens who file complaints in good faith is strictly prohibited under federal and Utah Anti-Retaliation/Whistleblower protection laws.
    b. Any individual found to have engaged in retaliation shall face disciplinary action, up to and including termination or censure.
4. Corrective Actions:
    a. If misuse is confirmed, appropriate corrective actions, including disciplinary measures, policy changes, or legal actions, shall be implemented.
5. Public Reporting:
    a. A summary of validated complaints and corrective actions taken shall be included in an annual public report, with all personally identifiable information redacted.

Section 17. Liability Mitigation and Public Trust

1. The formal process for employees and citizens to report concerns regarding misuse of sensitive records is found in "Section 6: Reporting Concerns Regarding Misuse of Sensitive Records" of this document.
2. The City Attorney shall review these policies annually to ensure compliance with state and federal laws and recommend updates as necessary.
3. The City Recorder shall compile an annual summary of privacy-related training completion rates, record classification updates, and data-sharing incidents for Council review and public transparency.

Section 18. This Ordinance shall be effective immediately upon its adoption and publication according to law.

PASSED, APPROVED, AND ADOPTED on the 28 day of May, 2025

Lake Point

By Alexis Wheeler
Chair

ATTEST:

City Recorder

SEAL

Voting:

Alexis Wheeler	Yea ✓	Nay ___	Absent ___
Jonathan Garrard	Yea ✓	Nay ___	Absent ___
Kirk Pearson	Yea ✓	Nay ___	Absent ___
Kathleen VonHatten	Yea ___	Nay ✓	Absent ___
Ryan Zumwalt	Yea ___	Nay ✓	Absent ___