Guideline
Non-personal Data

This guideline falls under A1477 Data and Information Management Administrative Policy.

Program Impacted	Civic Services *Edmontonians contribute to civic society and are engaged in promoting the quality of the community.* Technology & Data *The City of Edmonton's technology and data are leveraged to enable quality decision-making and enhance innovative service delivery.*
Approved By	Aileen Giesbrecht, City Clerk
Date of Approval	May 13, 2026
Approval History	N/A
Next Scheduled Review	November 13, 2026

Guideline Statement

This guideline provides guidance on the creation of non-personal data from personal information, the acceptable use and disclosure of non-personal data and the record-keeping requirements under the *Protection of Privacy Act* (POPA) when creating non-personal data.

This guideline falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy*.

Scope

This guideline provides recommendations to City of Edmonton employees, contractors, volunteers, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head. It applies to these parties whenever their work involves creating, collecting, receiving, accessing, using, disclosing, storing, maintaining, destroying, or transferring City records and information. All individuals listed above are responsible for protecting the privacy and confidentiality of personal information in accordance with POPA.

Guideline Description

This guideline provides direction on:

- the creation of non-personal data, including the required documentation,

- the assessment of non-personal data for risk of individual re-identification, and
- the protection of non-personal data.

Definitions

Aggregation is the process of grouping data, removing unnecessary details and summarizing it for analysis or reporting.

Blurring means the process of adding random noise to data values, such as age or date of birth, to reduce the risk of re-identifying individuals while keeping the data useful for analysis.

Bucketing is a form of aggregation that groups specific data values into broader categories.

Correlation criterion means the standard that must be met to ensure that individual records within a set of data (dataset) cannot be matched to other records about the same person found in separate datasets.

Data derived from personal information means data created by data matching that identifies any individual whose personal information was used in the data matching.

Hashing means a one-way process that uses a special algorithm to convert data of any size into a fixed-length string of characters, known as a hash value or digest.

Identifiers are pieces of data that are unique, or mostly unique, to an individual. Examples are name, personal telephone number and identification numbers such as Social Insurance Numbers (SIN) or Employee ID numbers.

Individualization criterion means the standard that must be met to ensure data does not allow a person to be isolated or distinguished from others within the dataset.

Inference criterion means the standard that must be met to ensure data does not allow personal information to be guessed or deduced from the data when combined with other available information.

Non-personal data means data, including data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual. This includes synthetic data.

Personal information means any recorded information about an identifiable individual, including but not limited to:

a) the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent;
b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
c) the individual's age, gender identity, sex, sexual orientation, marital status or family status;

d) an identifying number, symbol or other particular assigned to the individual;
e) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
f) information about the individual's health and health care history, including information about the individual's physical or mental health;
g) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
h) anyone else's opinions about the individual; and
i) the individual's personal views or opinions, except if they are about someone else.

Quasi-identifiers are pieces of data that may not identify an individual on their own, but a collection of quasi-identifiers could identify an individual. Examples of quasi-identifiers include home address, age, an anecdote about a person, family affiliations or professional associations.

Scrambling (magic numbers) refers to the process of using numbers to perform basic arithmetic operations on the input data to obscure the output data

Synthetic data means artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set.

Guideline Specification

Non-personal data is data that is changed so that an individual cannot be identified from it. To make individuals non-identifiable, creators of non-personal data use various methods, including but not limited to scrambling, hashing, aggregation and blurring.

Under the *Protection of Privacy Act (POPA)*, the City is only permitted to create non-personal data for the purposes of:

- research and analysis, and
- planning, administering, delivering, managing, monitoring or evaluating a program or service.

Aggregation of data for the *purpose of anonymization* is considered the creation of non-personal data. The following are actions taken under the *Access to Information Act* (ATIA) and are *not* considered the creation of non-personal data:

- redacting (blocking out or removing) identifiable information from a record before disclosing it in response to a request under ATIA,
- creating a summary or new record from existing unstructured data to help an applicant get the information they asked for (duty to assist) under ATIA, and

- proactively or routinely disclosing information or records deemed to be routinely available under section 90 of ATIA that have been filtered or edited to exclude personal identifiers to allow for disclosure.

Aggregation of any data for the *purpose of producing statistics and reporting numerical trends* is also not considered to be the creation of non-personal data.

Documenting the Creation of Non-Personal Data

The *Protection of Privacy Act, SA 2024, c P-28.5, s21(4)* specifies that the creation of non-personal data must be documented as a record that includes:

- a description of the *personal information* or *data derived from personal information* used to create the non-personal data,
- the purpose for creating the non-personal data,
- the method used for creating the non-personal data, and
- an assessment that confirms the identity of the individual, who is the subject of the non-personal data, cannot be identified or re-identified from the data.

This record will support the data itself and fall under the same retention and disposition schedule as the non-personal data.

Assessing Re-identification Risk

The creation or anonymization of personal information should be assessed against the following criteria to ensure that the non-personalized data truly protects privacy:

- *Correlation criteria: t*he assessment confirms that one cannot connect an individual's existing personal information across two or more separate datasets. If one could connect, then this criterion would not be met. For example, if one has a dataset with postal codes and information A, B, C and D and a second dataset with postal codes and resident names, you may be able to learn information A, B, C and D about those individuals by connecting the two datasets.
- *Individualization criteria*: the assessment confirms that one cannot single out or distinguish an individual from others within a dataset. If an individual could be singled out, then this criterion would not be met. For example, if a dataset has a single line with sufficiently rare combinations of demographic information or other quasi-identifiers, there is a reasonable chance that the individual could be identified.
- *Inference criteria:* the assessment confirms that one cannot infer or deduce new personal information about a person from the data, when combined with other publicly available information. If one could infer or deduce, then this criterion would not be met. For example, guessing information from publicly available sources might occur if the information includes links to other sources, such as residential

addresses, which can be associated with owners/residents and reveal additional personal information about them.

Assessments are based on an assumption of reasonableness, meaning an individual with average technical skill, access and means should not be able to identify or distinguish an individual using ordinary (non-criminal) methods.

It is unnecessary to show there is zero risk of re-identification; however, the assessment results must show that the residual risks of re-identification are very low. Assessments need to consider context, including:

- the circumstances related to the anonymization of personal information, in particular, the purposes for which the public body intends to use the anonymized information,
- the nature of the information,
- the correlation, individualization and inference criteria,
- the measures required to re-identify the individual, taking into account the efforts, resources and expertise required to implement those measures.

Protecting Non-personal Data

Security Measures

Non-personal data must be protected by reasonable safeguards against risks such as unauthorized access, collection, use, disclosure or destruction. This includes classifying non-personal data in accordance with the *City of Edmonton Classification and Retention Schedule* and implementing appropriate safeguards in alignment with City of Edmonton policy tools.

If non-personal data is created by an automated system, human auditing and validation measures must be in place to ensure the data's accuracy and reliability.

Disclosure

Non-personal data may be disclosed to another public body — for example, to another municipality, a school board or the Government of Alberta — for any purpose.

The City of Edmonton will disclose non-personal data to an individual outside of the corporation only for the following purposes:

a) research and analysis, and/or
b) planning, administering, delivering, managing, monitoring or evaluating a program or service.

Disclosure may occur only after the outside individual signs an agreement that complies with the *Creation and Protection of Non-personal Data Administrative Standard.* Checking a box to agree to terms and conditions constitutes such an agreement.

Compliance

All City of Edmonton employees, contractors, volunteers, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head are responsible for maintaining the privacy and confidentiality of information in accordance with POPA. Branch managers are accountable for ensuring that privacy practices within their branches comply with legislation and City of Edmonton policies, including the *Corporate Records and Information Management Accountability Model (RASCI)*. Failure to comply with this guideline could result in the loss of personal information, damage to the City of Edmonton's reputation, costs and fines, increased legal risk, information breaches and complaints from the public.

References and Supporting Resources

Legislation

- *Protection of Privacy Act, SA 2024, c P-28.5*
- *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025*
- *Protection of Privacy Regulation, Alta Reg 132/2025*
- *City Administration Bylaw, Bylaw 16620*
- *A1477 Data and Information Management Administrative Policy*

Supporting Resources

- City of Edmonton Delegation of Authority Order
- Corporate Information Management Glossary of Terms
- Corporate Records and Information Management Accountability Matrix (RASCI)
- Creation and Protection of Non-personal Data Administrative Standard