AD.1.1.1 Personal Information Procedure
Schedule D: Non-Personal Data and Data Matching Guidelines

PHILOSOPHY

SAIT will create, use, protect, and disclose non-personal data and/or engage in data matching activities only for authorized institutional purposes and in accordance with the *Protection of Privacy Act (POPA)* and applicable SAIT policies and procedures.

DEFINITIONS

Aggregated data	Information that is collected and compiled into a summary or grouped format, typically for the purposes of reporting and analytics.
Anonymized data	Data that has been processed to permanently remove or alter personally identifiable information, for example, names, addresses, and social insurance numbers. This process of de-identification ensures that the data cannot be linked back to any specific individual, even when combined with other data, while still preserving the data for analysis or other purposes.
Data custodian	The 'system owner' who manages the storage, access, transport, and safety of the actual data. They support data stewards in implementing technology changes and granting access. They maintain the technical infrastructure of SAIT systems, implementing access rights and controls to ensure the accuracy, integrity, security and privacy of data in SAIT's custody. A data custodian works with data stewards to ensure data-related issues are escalated to the appropriate governing body in a timely manner.
Data derived from personal information	Data created by data matching that identifies any individual whose personal information was used in the data matching. It must involve the merging of two or more sources to create new information about an individual; The personal information in the data remains identifiable.
Data matching	Refers to the linking of personal information across two or more databases, or other electronic data sources, to generate data derived from personal information. Such data identifies any individual whose personal information was utilized in the data matching process.

Disaggregated data	Information that is broken down into detailed sub-categories for the purposes of understanding gaps, underlying trends, patterns or insights not observable in aggregated data sets.
Non-personal data	Data derived from personal information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the *Protection of Privacy Act (POPA).*
Personal information	Recorded information about an identifiable individual and includes, but is not limited to, name, residential address and phone number, personal email address, sex (sex assigned at birth), age, gender identity, title, pronouns, sexual orientation, marital or family status, religious affiliation, indigeneity, ethnicity, disability status, languages spoken, immigration status, identification number, education and employment history, health information including documentation of approved accommodations for physical or mental disability, an individual's personal views or opinions and information about an individual's financial matters.
Privacy impact assessment	A document used for information systems, administrative practices and policy proposals that helps to identify and address potential privacy risks that relate to the collection, use or disclosure of individually identifying personal or health information.
Public body	An organization that is under the jurisdiction and oversight of the Government of Alberta but does not include federal public bodies or private corporations, not-for-profit organizations and/or public bodies outside of Alberta.
Reasonable security arrangements	Practical measures, proportionate to risks, designed to protect non-personal data from unauthorized access, use, disclosure, or destruction.
Research data	Data collected, observed, generated or created from research and/or scholarly activity used to validate research findings.
Synthetic data	Artificial data generated by computer to maintain the structure and patterns of real data without being linked to any individual in the original dataset.

A. Creation and Use of Non-Personal Data

1. SAIT will only create non-personal data from personal information which is already in SAIT's custody or control, and only for the following purposes:

   a) Research and analysis;

   b) Planning, administering, delivering, managing, monitoring, or evaluating a program or service; and

   c) Other prescribed purposes as authorized through the *POPA* and its associated regulation.

2. This schedule does not apply to non-personal data where it is being created or used solely to support SAIT's internal day-to-day operational, administrative, quality assurance, reporting and/or institutional decision-making activities, where:

   a) The school or department who will be creating and using the non-personal data, and/or engaging in data matching activities, is also the owner or custodian of the source personal information; and

   b) The resulting data is used exclusively within SAIT and will not be disclosed to any individual or group external to SAIT (including but not limited to disclosures for government and/or regulatory reporting requirements).

   The creation, use and disclosure of such data are governed by SAIT's data governance, privacy, information management and records management policies and procedures, as applicable.

3. Where non-personal data is created for purposes other than those outlined above and/or where it will be disclosed to external parties, the SAIT employee requesting the data, or the SAIT school/department responsible for its creation, must submit a Non-Personal Data Creation form (NPD form). Refer to the Non-Personal Data Creation Guide and decision tree at the end of this document for more information.

4. The Access and Privacy Unit, Office of General Counsel, will review NPD form submissions to determine whether a privacy impact assessment (PIA) is required, in accordance with procedure AD.1.1.2 Privacy Impact Assessment.

5. The creation and/or use of non-personal data for research purposes must additionally meet the requirements of procedure AD.3.3.2 Research Data Management.

6. SAIT is committed to protecting the privacy of individuals by ensuring that any methods used to create non-personal data prevent identification or re-identification of individuals. Non-

personal data generated by SAIT may be utilized for any institutional purposes, provided that the requirements of section A of this schedule are met and that the identity of any individual who is the subject of the non-personal data remains unidentifiable and cannot be reidentified from the data.

B. Protection of Non-Personal Data

1. Data custodians must ensure reasonable security arrangements are taken to protect non-personal data at rest and in-transit, such as, for example, the encryption of data and implementing strong access controls with multi-factor authentication.

2. The Information and Technology Services department (ITS) will complete regular security assessments and updates of systems where non-personal data is stored, in alignment with institutional cybersecurity strategies and data backup protocols.

3. Any member of the SAIT community can report an instance where non-personal data was or is at risk of being compromised or disclosed in an unauthorized manner in accordance with SAIT's established privacy incident response process outlined in AD.1.1.3 Privacy Incident Response procedure.

4. All non-personal data must be securely stored in compliance with SAIT's privacy, data governance and information management policies and procedures.

5. Records containing non-personal data will be retained in accordance with SAIT's Classification Scheme and Records Retention Schedule (refer to procedure AD.3.2.3 Retention and Disposition Schedule).

C. Disclosure of Non-Personal Data

1. SAIT may disclose non-personal data to other public bodies for any purpose without restriction, provided the guidelines regarding the creation and protection of non-personal data outlined in sections A and B of this schedule have been followed.

2. All disclosures of non-personal data and/or data derived from personal information must adhere to the data classification and security requirements set out in procedure AD.3.3.1 Data Governance and procedure AD.3.3.2 Research Data Management for research datasets.

3. Non-personal data may only be disclosed in disaggregated form to individuals or organizations other than public bodies if:

    a) The purpose aligns with authorized uses as defined in section A.1 of this schedule.

b) A signed agreement is in place that includes compliance with the *POPA*, its associated regulations, and SAIT policies and procedures; and

c) The dean/director or designate of the applicable school/department, in which the non-personal data was created, authorizes the conditions related to its use and disclosure, including:

i) Confidentiality;

ii) Data security and retention;

iii) Prohibition of re-identification; and

iv) Prohibition of subsequent use or disclosure.

4. Subsequent use or disclosure of non-personal data to external parties for a purpose which differs from its original intent requires a revised or new signed agreement approving the additional conditions and includes authorization from dean/director or designate of the applicable school/department in which the non-personal data was created.

5. SAIT may disclose aggregate or statistical reports containing non-personal data without restriction, provided such data cannot be used to identify individuals.

D. Data Matching

1. Data matching may use only personal information that SAIT has obtained from another public body or information that is already within its custody or control. SAIT will ensure data matching is only conducted for authorized purposes, in accordance with POPA, and in a manner that minimizes privacy risk by limiting use, safeguarding personal information and preventing unauthorized disclosure, retention or reuse of derived data.

2. Any new or substantial change to a practice, program, project or service that involves data matching between two or more public bodies requires a privacy impact assessment (PIA) to be prepared. SAIT employees involved in such initiatives and projects must request the required PIA through the Third-Party Risk and Privacy Assessment Request form in ServiceNOW.

3. Data matching is only permissible where the rationale for combining the sources of data aligns with one or more of the following purposes:

a) Research and analysis;

b) Planning, administration, delivery, management, monitoring or evaluation of a program or service; and/or

c) One or more prescribed purposes as outlined in the *Protection of Privacy Act* (POPA) and *Regulation*.

4. Personal information must not be collected directly from the individual to whom the data pertains for the purpose of data matching.

5. Employees involved in data matching are required to implement reasonable security arrangements to safeguard any data derived from personal information against privacy risks such as unauthorized access, collection, use, disclosure or destruction.

6. Data created through data matching may only be used for the purpose for which it was generated and must be either destroyed or transformed into non-personal data, once that purpose has been fulfilled.

7. The disclosure of data derived from personal information is strictly prohibited, except when such disclosure involves sharing the data with the public body that originally provided the personal information used in the creation process.

ASSOCIATED DOCUMENTS:

- Non-Personal Data Creation Form
- Non-Personal Data Creation Guide
- Non-Personal Data Decision Tree

Non-Personal Data and Data Matching Decision Tree: