



## RESEARCH AGREEMENT

between

**Simon Fraser University (the “University”)**

and

[ \_\_\_\_\_ ] (the “Researcher”)

### Collection Notice

The information on this form is collected under the authority of the *Freedom of Information and Protection of Privacy Act* (FIPPA). It is related directly to and needed by the University to provide you with access to archival records containing third party personal information for research purposes. The information will be used to make a decision about your application and, if approved, used to ensure your compliance with the terms and conditions of the Agreement. If you have any questions about the collection and use of this information, please contact the University Archivist in the Archives and Records Management Department at [archives@sfu.ca](mailto:archives@sfu.ca).

### Purpose of the Research Agreement

*See Schedule 1 for definition of terms*

This Agreement is required to request access to, and authorize disclosure of, university or private records for research or statistical purposes. The records covered by this Agreement may contain personal information that is subject to restrictions as stipulated in a deed of gift, donation agreement, *The Freedom of Information and Protection of Privacy Act*, RSBC 1996, ca.165 (“FIPPA”), or Archives’ policy. This Agreement is a legally binding contract between the Researcher and the University.

*Archives use only*

Research Agreement # \_\_\_\_\_ Approved date \_\_\_\_\_

FOI Access Request # \_\_\_\_\_ Expiry date \_\_\_\_\_

Type of records  University records  Processed records  Sensitive PI  
 Private records  Unprocessed records  Non-sensitive PI

Applicable statute, agreement or policy  FIPPA  Donor agreement  Policy

## PART A – Identification of Researcher

Name \_\_\_\_\_

Street address \_\_\_\_\_

City / town \_\_\_\_\_

Province \_\_\_\_\_

Country \_\_\_\_\_

Postal code \_\_\_\_\_

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Institutional  
Affiliation

(if applicable) \_\_\_\_\_

*\*It is the applicant's responsibility to notify the SFU Archives and Records Management Department of any change in contact information during the duration of this agreement.*

## PART B – Description of research project

1. Requested expiry date for this agreement \_\_\_\_\_.

Answer the following question on a separate page and attach it to this form.

2. Provide an overview and general description of your research project, including (a) research purpose, (b) proposed methods of analysis, (c) anticipated research products, and (d) why your research requires access to records that include personal information (see the definition of personal information in Schedule 1). The stated research purpose must demonstrate a clear and substantive relationship to the records for which access is requested. Access to records containing personal information shall not be granted where such a relationship is absent or has not been adequately demonstrated, as determined by the University Archivist.

Attach the following additional information:

3. List the records to which you are requesting access under this Research Agreement; attach separately or use Schedule 2 of this form.

## PART C – Agreement on terms and conditions of access

I, the Researcher, understand and agree to the following terms and conditions:

### Use and disclosure of personal information

1. I will not use the personal information disclosed through the records for purpose of contacting a person.

2. This research project does not involve data-linking (see definitions in Schedule 1).
3. I will not disclose personal information contained in the records described in Schedule 2 to the individual(s) to whom it relates.
4. I will not use or disclose personal information contained in the records for any purpose other than as described in Part B, nor any subsequent purpose without the express written permission of the University Archivist.

*An example is the reuse of personal information in a way not originally envisioned in your current research project. This includes re-using personal information in a follow-up research project that grows out of your current one.*

5. I will not write or prepare reports, papers, presentations, theses, or any other works that describe the results of the research undertaken in such a way that individuals in the requested records can be identified. This includes combining personal information found in the requested records with personal information that is publicly available from other sources that could serve to identify individuals. There will be no exceptions to this rule without prior written permission from the University.
6. I acknowledge that it is possible to identify an individual by a combination of characteristics or variables, even if that person is not named. Therefore, de-identification may require more than simply removing names (i.e., anonymization). For example,

*Many people might well know who is being discussed if mention is made of a tall female gas station attendant in Prince Rupert who is 35 years old and born in Kelowna, B.C.*

*An employee's action causes public controversy and there are accounts in the newspapers. A researcher finds detailed evaluations of the employee's work performance in a case file. In publishing the research, the case is described but the employee's identity is concealed. Nevertheless, it is possible to combine the description of the case with the media accounts to render the employee identifiable.*

### **Security and confidentiality**

7. I understand that I am responsible for maintaining the security and confidentiality of all personal information found in or taken from these records.
8. Apart from me, only supervisors or research project members working on this research project will have access to this personal information in a form which identifies or could be used to identify the individual(s) to whom it relates.
9. Before any personal information is disclosed to the individuals referred to in section 4, I will ensure they understand and undertake that they will not disclose the information to any other person and that they will ensure compliance with all terms and conditions of this Agreement. I will provide them each a copy of this Agreement.
10. If any of the records subject to this agreement are lost, stolen, or accessed in a manner not compliant with this agreement, I will notify the University Archivist as soon as possible.
11. Each project member will have an individual and unique Strong Password (if applicable). The researchers will ensure the computer systems are equipped with access logs to help identify who has accessed the data.
12. I will not transmit unsecured (e.g., unencrypted) personal information that identifies or could be used to identify the individual(s) to whom it relates by means of any telecommunications/data device, including telephone, fax, or email.

## Removal or Destruction of Individual Identifiers

13. I will remove or destroy individual identifiers associated with the records in any copies I receive of the records or in my notes about them. I will do this at the earliest time at which removal or destruction can be accomplished consistent with the research purpose. At the latest, this will occur on the expiry of this Agreement. The University Archivist must approve any extension to this time in writing.
14. I will file a statement with the University Archivist certifying that such removal or destruction has taken place within two weeks of the expiry of this agreement. The University Archivist must approve any extension to this time limit in writing.
15. I will remove individual identifiers in a manner that ensures that remaining personal information (including any found in research notes) cannot be used to identify the individual to whom it relates. If necessary, I will destroy copies of requested records or data in their entirety. All destruction or removal of individual identifiers will be confidential and complete in order to prevent access or reconstruction by any unauthorized persons.

The following methods of destruction are acceptable:

**Paper records:** Paper records, at a minimum, must be destroyed by “cross-cut” shredding. Other acceptable methods of destruction are incineration, hammer-mill shredding, or pulverizing.

**Electronic records:** Electronic records must be destroyed in such a way that the data is permanently deleted and there is no possibility to recover or reconstruct the data from the digital storage device. Note that standard deletion on a computer does not erase the data, it merely frees up disk storage space so that it may eventually be overwritten; the data is still recoverable. Secure delete means that the data is overwritten immediately so that it cannot be reconstructed.

16. I understand that I am responsible for ensuring complete compliance with the terms and conditions of this Agreement, the University’s policies and procedures relating to the confidentiality of personal information and, if I am accessing university records, FIPPA.
17. In the event that I become aware of a breach of any of the conditions of this Agreement, I will immediately notify the University Archivist in writing.
18. I agree and understand that the expiry date for access to the records is the date listed in section B.1 of this Agreement unless otherwise agreed to in writing by the University Archivist.
19. In order to add additional records after approval of this Agreement, I must list the records in a separate, dated and approved addendum that I will submit to the Archives and Records Management Department for review, and which may require an additional delegated authority approval.
20. Where required by law, where necessary to protect personal information, or in response to any actual or suspected breach of this Agreement, the University may, at its sole determination: (a) demand the immediate return of all copies of records, in any form, (b) revoke or suspend the Researcher’s access to records without prior notice, (c) impose an immediate publication hold on any Research Product arising from the use of these records until the University has completed a privacy and compliance review and verified, to its satisfaction, that no personal information has been disclosed by the Research Product in breach of FIPPA, and (d) conduct an assessment or investigation under the authority of Responsible Conduct of Research Policy (R60.01).
21. This Agreement does not waive my requirement to seek ethics approval as may be required for the research contemplated by this Agreement.

*By signing this Agreement, the Researcher assumes and takes responsibility and liability for and shall indemnify and hold Simon Fraser University (SFU) its members, managers, employees, and agents harmless from the following: (a) any and all liabilities related to the Researcher failing to adhere to the Terms and Conditions of Access as detailed in Part C of this agreement.*

\_\_\_\_\_  
Signature of Researcher

\_\_\_\_\_  
Date

\_\_\_\_\_  
[Print Name]

**PART D – Approval of terms and conditions of access**

This research agreement applies to the records listed and described in Schedule 2. These records are in the custody and control of the University Archives. The University Archivist has been delegated authority to approve these agreements by the University's Information Policy I10.02.

\_\_\_\_\_  
Signature of University Archivist

\_\_\_\_\_  
Date

\_\_\_\_\_  
[Print Name]

The terms and conditions of this Agreement are hereby approved.

## SCHEDULE 1 – Definition of terms

<b>Anonymize</b>	<p>Present the results of research in such a way that individuals whose personal information is contained in the requested records cannot be identified, and no linkages can be made between any personal information found in the requested records and personal information that is publicly available from other sources.</p> <p>Under this research agreement you are required to anonymize the results of your research. See Part C, paragraphs 12 to 14.</p>
<b>Contact information</b>	<p>Information that enables an individual at a place of business to be contacted; includes name, position title, business telephone number, business address, business email or business fax number of the individual.</p>
<b>Data linking</b>	<p>Means the linking or combining of personal information in one source with personal information in one or more other sources. (see <i>FIPPA</i>, Schedule 1).</p> <p>Systematic comparison of sets of information, usually found in information banks or data banks; "information banks" include paper case files as well as electronic databases. (See <i>FIPPA Policy and Procedures Manual</i>: s. 33, formerly s.35).</p> <p>Under the FIPPA Act (s. 33(3)(h)(iii)), data linking is permissible for research purposes if it is not harmful to the individual and the benefits to be derived from the research is clearly in the public interest. "Research purposes" in this context means study of sources to ascertain facts or verify theories with no intention of making decisions about the record subjects' rights or privileges.</p> <p>Under this research agreement you may access the records requested for purposes of data linking, but you must clearly describe this in Part B, and you must anonymize the results of your research in any research products. See Part C, paragraph 11.</p>
<b>Disclose</b>	<p>Reveal, show, expose, provide copies of, sell, give or tell (see <i>FIPPA Act Policy and Procedures Manual: Definitions</i>).</p> <p>You cannot disclose any personal information contained in the records to which you have been given access under the terms and conditions of this research agreement. See Part C, paragraphs 10 and 17.</p>
<b>Individual identifier</b>	<p>Information that would enable a third party to deduce the identity of the person concerned; examples include a person's name, Social Insurance Number, student number, employee number, address, date of birth (usually used in combination with other identifiers); see <i>FIPPA Act Policy and Procedures Manual</i>: s. 33, formerly s.35.</p> <p>Under this research agreement you are required to destroy or remove all individual identifiers from any copies of the records requested and from your notes; you must provide a date by which this will be done by the latest. See Part C, paragraphs 18 and 19.</p>

**Personal information**

Recorded information about an identifiable individual, other than business contact information, including but not limited to:

- names, home addresses and telephone numbers;
- age;
- sex;
- marital or family status;
- identifying number;
- race, national or ethnic origin;
- colour;
- religious or political beliefs or associations;
- educational history;
- medical history;
- disabilities;
- blood type;
- employment history;
- financial history;
- criminal history;
- images;
- anyone else's opinions about an individual;
- an individual's personal views or opinions; and,
- name, address and phone number of parent, guardian, spouse or next of kin.

**Sensitive Personal information**

Personal information may be considered sensitive depending on a) the type of information, and b) the context in which it is collected, used, disclosed or stored. The following is a non-exhaustive list of types of personal information that are commonly considered sensitive:

- Personal health information
- Genetic and biometric data
- Personal financial information
- Geolocation data
- Criminal records
- Racial or ethnic origin
- Sexual orientation
- Religious, philosophical or political belief

**Research product**

Any work that present the results of your research. Includes reports, presentations, websites, papers, articles, theses, books, graphics, audio recordings, and audio-visual works.

You must describe your anticipated research products in Part B, paragraph 2.

**Strong password**

A password that consists of 12 or more characters and includes uppercase and lowercase letters, numbers, and symbols.

