**McMaster Preliminary Analysis Questionnaire**

**Instructions:** *Delete these instructions after completion*

* The Preliminary Analysis is the first step of the Privacy Impact Assessment (PIA).
* Complete Part 1 of this questionnaire to determine if your project will involve personal information – if yes, complete Part 2.
* Enter your answers in the space provided and attach additional material, as needed. Text boxes expand as needed.
* Reference the footnotes for clarification of a term or for information about supporting resources.
* Submit your completed Preliminary Analysis Questionnaire, along with any supplementary information (e.g., background about your project, etc.), to the University Secretariat Office / Privacy Officer at [univsec@mcmaster.ca](mailto:univsec@mcmaster.ca)
* If you have any questions about the Preliminary Analysis Questionnaire or the PIA process, contact the University Secretariat Office at 905-525-9140 ext. 2433

Adapted from the Ontario Public Service (OPS) Preliminary Analysis Questionnaire

**Important Contacts:**

University Secretariat

[univsec@mcmaster.ca](mailto:univsec@mcmaster.ca)

(905) 525-9140 x24337

<http://www.mcmaster.ca/univsec/index.cfm>

Office of Legal Services

<http://www.mcmaster.ca/ols/>

IT Security - UTS

[c-it-security@mcmaster.ca](mailto:c-it-security@mcmaster.ca)

(905) 525-9140 x28299

<http://www.mcmaster.ca/uts/security/ITsecurity/index.html>

**McMaster Preliminary Analysis Questionnaire**

**McMaster Preliminary Analysis Questionnaire**

**Privacy Impact Assessment**



**Part 1**

1. **Project and Institution**

|  |  |
| --- | --- |
| **Project / Protocol Title** |  |
| **Department / Faculty** |  |
| **Program** |  |
| **Project Sponsor** |  |
| **Data/Service Owner**[[1]](#footnote-1) |  |

1. **Contact Information[[2]](#footnote-2)**

|  |  |
| --- | --- |
| **Name** |  |
| **Title (of contact)** |  |
| **Department/Faculty** |  |
| **Phone Number** |  |
| **E-mail** |  |

1. **Project Description[[3]](#footnote-3)**
   1. **Describe your project, including its purpose (e.g., development of service, research activity, RFP/RFS, etc.), scope (e.g., pilot, study, part of larger project, etc.) and key objectives. Attach relevant documentation such as Research Protocol, if needed as appendices.**

|  |
| --- |
| Enter description here |

1. **Data Collection, Use and Disclosure**
   1. **Identify the kinds of data involved in the program, service, system or other application resulting from your project (check “X” all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| No data or records[[4]](#footnote-4) (Please explain how and why in row below) |  |  |  |
| Enter explanation here | | | |
| Information about individuals acting in their personal capacity |  |  |  |
| Information about individuals acting in their business, professional or official capacity (e.g., name and job title, business contact information) |  |  |  |
| Information about organizations (e.g., companies, not-for-profit organizations, government institutions) |  |  |  |
| Aggregated, anonymized or otherwise de-identified[[5]](#footnote-5) information (Please outline in the row below the process how that is done and why it is not possible to identify/re-identify individuals from that data) |  |  |  |
| Enter process here | | | |

* 1. **Identify the kinds of personal information[[6]](#footnote-6) that will/may be collected, used and disclosed?[[7]](#footnote-7) (check “X” all that apply)**

|  | **Collect** | **Use** | **Disclose** |
| --- | --- | --- | --- |
| No personal information |  |  |  |
| Unknown at this time (Please explain why in row below) |  |  |  |
| Enter explanation here | | | |
| Name |  |  |  |
| Personal address |  |  |  |
| Personal email address |  |  |  |
| Personal telephone number |  |  |  |
| Race |  |  |  |
| National origin |  |  |  |
| Ethnic origin |  |  |  |
| Skin colour |  |  |  |
| Religion |  |  |  |
| Age |  |  |  |
| Date of birth |  |  |  |
| Sex |  |  |  |
| Sexual orientation |  |  |  |
| Marital status |  |  |  |
| Family status |  |  |  |
| Education |  |  |  |
| Criminal history |  |  |  |
| Employment history |  |  |  |
| Financial transactions involving the individual |  |  |  |
| Medical information including health card number, medical history, psychiatric history, medication history, laboratory test results, diagnostic images, immunization records, and any other health information related to identifiable individuals |  |  |  |
| Psychiatric history |  |  |  |
| Identifying number including personal identification number, client or licence number, Health Card number, social insurance number, student number, bank card number (credit or debit), bank account number, or other type of unique identifying number related to identifiable individuals |  |  |  |
| Identifying symbol (e.g. signature, professional designation, or an emblem ) |  |  |  |
| Photograph of the individual |  |  |  |
| Other identifying particulars of the individual, including identifying physical characteristics such as eye colour, tattoo or scar[[8]](#footnote-8) |  |  |  |
| DNA, fingerprints or other biometric (e.g., handprint, iris scan, voiceprints, etc.) |  |  |  |
| Blood type |  |  |  |
| Personal opinions or view of the individual, except where they relate to another individual |  |  |  |
| Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence |  |  |  |
| Views or opinions of an individual about another individual |  |  |  |
| Other types of personal information not listed above (Please list specifics in row below) |  |  |  |
| Enter other types here | | | |
| Other types of information that either alone or in combination with other data are reasonably likely to enable the identification or location of an individual (e.g., geospatial data, Internet Protocol (IP) address, transaction logs, web analytics tracking) (Please list specifics in row below) |  |  |  |
| Enter other types here | | | |

|  |  |
| --- | --- |
|  | If you checked “No personal information” will be collected, used or disclosed, and your project will NOT involve personal information, as identified in Question 4.2 list, you do not need to complete Part 2 of the questionnaire.  Submit your Preliminary Analysis questionnaire to IPA via [univsec@mcmaster.ca](mailto:univsec@mcmaster.ca) |
|  | If your project WILL INVOLVE personal information or it is **Unknown at this time**, as identified in Part 1, Question 4.2, you need to complete Part 2 of this questionnaire.  Continue to next page  *Delete these instructions after completion* |

**Part 2**

|  |
| --- |
| **Note:** To be completed ONLY by projects that will involve personal information, as identified in Part 1, Question 4.2 of this questionnaire |

1. **Project Authority** 
   1. **Describe the authority for your project (cite specific Research Ethics Clearance, legislation and section numbers, memoranda of understandings, agreements, contracts or other relevant instruments)**

|  |
| --- |
| Enter description here |

1. **Privacy Legislation**
   1. **Identify applicable privacy legislation (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Freedom of Information and Protection of Privacy Act |  |  |  |
| Municipal Freedom of Information and Protection of Privacy Act |  |  |  |
| Personal Health Information Protection Act |  |  |  |
| Personal Information Protection and Electronic Documents Act |  |  |  |
| Payment Card Industry Data Security Standard |  |  |  |
| Canadian Anti-Spam Legislation |  |  |  |
| Other (please identify relevant statutes in row below) |  |  |  |
| Enter other here | | | |
| None – not covered by privacy legislation (please explain in row below) |  |  |  |
| Enter explanation here | | | |

* 1. **Identify if your project will involve the following types of personal information**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Personal information that will be excluded from the application of FIPPA under section 65[[9]](#footnote-9) |  |  |  |
| Personal information that will be maintained for the purpose of creating a public record[[10]](#footnote-10) |  |  |  |

1. **Data Subject** 
   1. **Identify whom the personal information will relate to (i.e., data subjects) (check all that apply)**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **No** | **Unknown** |
| Public |  |  |  |
| Students |  |  |  |
| Staff / Faculty |  |  |  |
| Retirees |  |  |  |
| Alumni |  |  |  |
| Others (Please describe in row below) |  |  |  |
| Enter description here | | | |

1. **Project Characteristics**
   1. **Identify key characteristics of your project? (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Involves creation of new program, process, service, technology, information system or other type of IT application |  |  |  |
| Involves change to existing program, process, service, technology, information system or other type of IT application |  |  |  |
| Involves procurement of goods or services |  |  |  |
| Involves outsourcing or contracting for service related to the collection, use, disclosure, processing, retention, storage, or disposal of personal information |  |  |  |
| Involves development of Request for Proposal or Services |  |  |  |
| Involves a process, system or technology that will have significant privacy implications for individual privacy or the protection of personal information (e.g., use of surveillance system or biometrics) |  |  |  |
| Involves a process, system or technology for which the privacy risks are not known or well documented (e.g., technology new to McMaster University) |  |  |  |
| Involves program, system or technology that is reasonably likely to have university-wide impact |  |  |  |
| Involves the creation of an information system or database containing personal information, including matching, merging, combining or centralizing of databases |  |  |  |
| Involves the sharing, including sale, of personal information |  |  |  |
| Involves data warehousing or data marts |  |  |  |
| Involves the need to identify, authenticate or authorize users – public, students, staff, faculty (e.g., public key infrastructure, identity and access, identity cards, biometrics, passwords, 2-factor authentication, digital signatures, multi-purpose identifiers, or use of other authentication technology) |  |  |  |
| Other (Please specify project characteristic row below) |  |  |  |
| Enter other here | | | |

* 1. **Identify changes that will result from your project (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Involves a change in data/service owner |  |  |  |
| Involves a change to legislative authority (i.e. compliance requirement, FIPPA to PHIPA) |  |  |  |
| Involves a change in users of process or system (eg., public, students, staff, faculty, etc) |  |  |  |
| Involves a change in partners or service providers |  |  |  |
| Involves a change in the amount or type of personal information, or the process by which it is collected, used, disclosed, retained, secured, and disposed of |  |  |  |
| Involves a change to the purposes for which personal information was collected, used or disclosed |  |  |  |
| Involves a change from direct to indirect collection of personal information[[11]](#footnote-11) |  |  |  |
| Involves a change in roles and responsibilities (i.e., who can do what, when, where, why and how with personal information) |  |  |  |
| Involves a change in the sharing, including sale, of personal information with other programs, institutions, government, partners, or 3rd parties |  |  |  |
| Involves a change to, or eliminating of, existing opportunities for anonymity or pseudonymity |  |  |  |
| Involves a change in the technology used to collect, process, transport, disclose personal information (i.e., hardware and software) |  |  |  |
| Involves a change to an information system or database containing personal information, including matching, merging, combining or centralizing of databases and data marts and warehouses |  |  |  |
| Involves a change of medium or service delivery channels (e.g., automation of manual process, conversion from paper to electronic records, creation of new website to provide services to clients) |  |  |  |
| Involves a change in the security requirements or measures |  |  |  |
| Other (Please specify change or proposed change in row below) |  |  |  |
| Enter other here | | | |

* 1. **Describe your project’s current project phase. For example, initial, project planning, implementation, operational. Provide commencement, completion dates and milestones if available.**

|  |
| --- |
| Enter description here |

1. **Technology**

* 1. **Identify technology-related characteristics of your project known at this time (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Involves technology designed to monitor, track or observe an individual or their transactions (e.g., video cameras, cell phones, geospatial or location-based services) |  |  |  |
| Involves logging information, usage or preferences (e.g., IP addresses, traffic data, access or transaction logs, cookies, or mechanism for recording individual’s use of system/service) |  |  |  |
| Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media such as Facebook, Twitter, Instagram, etc |  |  |  |
| Involves technology systems that through their use may collect, transmit or store potentially personal information (e.g., email, messaging, video conference, desktop collaboration/sharing, etc.) |  |  |  |
| Involves processing or storing of personal information in virtual environment (e.g., Cloud computing/storage) |  |  |  |
| Involves use of analytics or performance measurements (e.g., web analytics, social media analytics, business intelligence tools) |  |  |  |
| Involves the acquisition of, or customization of, commercial software, hardware or IT support services by external vendors (e.g., Commercial-of-The-Self (COTS) products) |  |  |  |
| Involves the development of, or customization of, software, hardware or IT support services by university resources (e.g., UTS) |  |  |  |
| Involves creation of information system or other type of IT application that will be populated by others (e.g., survey systems like LimeSurvey) |  |  |  |
| Involves system or application that will automatically collect or disclose personal information (eg., collect IP address or other potential personal information) |  |  |  |

1. **Partners/Service Providers[[12]](#footnote-12)**
   1. **List all departments/faculties/3rd parties involved in the development or implementation of your project[[13]](#footnote-13)**

|  |  |  |
| --- | --- | --- |
| **Administration** | **Faculty/Research** | **3rd Party** |
|  |  |  |

* 1. **List all departments/faculties/3rd parties that will collect, use/process, disclose, retain, store, secure or dispose of personal information on behalf of the data/service owner**

|  |  |  |
| --- | --- | --- |
| **Administration** | **Faculty/Research** | **3rd Party** |
|  |  |  |

* 1. **Identify any location outside of Ontario where personal information may be retained or stored[[14]](#footnote-14)**

|  |
| --- |
| Enter locations here |

* 1. **List all departments/faculties/3rd parties that will have access to, or use, the personal information**

|  |  |  |
| --- | --- | --- |
| **Administration** | **Faculty/Research** | **3rd Party** |
|  |  |  |

* 1. **List all organizations that will be needed to manage or maintain the process, system, service or application involving personal information**

|  |  |  |
| --- | --- | --- |
| **Administration** | **Faculty/Research** | **3rd Party** |
|  |  |  |

* 1. **Identify how service providers/3rd party will be bound to follow relevant privacy and security requirements (check all that apply)**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **In Place** | **Being Developed** | **Unknown** |
| Contracts |  |  |  |
| Memoranda of Understanding |  |  |  |
| Agreements (non-disclosure or service level) |  |  |  |
| Other (Please explain in row below) |  |  |  |
| Enter explanation here | | | |

1. **Consultation**
   1. **Identify with whom you have consulted regarding the privacy implications of your project**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| University Secretariat[[15]](#footnote-15) |  |  |  |
| Legal Counsel[[16]](#footnote-16) |  |  |  |
| Research Ethics Board (MREB/HiReb) |  |  |  |
| IT Security - UTS[[17]](#footnote-17) |  |  |  |
| IT Department - other (list faculty/department below) |  |  |  |
| Enter other here | | | |
| Office of the Information and Privacy Commissioner |  |  |  |
| Other (Please identify who in row below) |  |  |  |
| Enter other here | | | |

1. **Stakeholders**
   1. **Indicate if you anticipate a negative reaction to your project from the following**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Public |  |  |  |
| Students |  |  |  |
| Staff |  |  |  |
| Faculty |  |  |  |
| Media |  |  |  |
| Other (Please specify in row below) |  |  |  |
| Enter other here | | | |

1. **PIA Activities**

**13.1 Describe PIA activities (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Completed PIA process |  |  |  |
| Updating previous PIA documents related to project |  |  |  |
| Planning to continue PIA process |  |  |  |
| Engaging University Secretariat to assist in completing PIA documents |  |  |  |
| Engaging IT Security - UTS resource to assist in IT security control determination |  |  |  |
| Engaging Purchasing to assist with negotiating terms of service contract |  |  |  |
| Engaging Office of Legal Services to assist in service contract language |  |  |  |
| Not planning to continue PIA process (please explain why in row below) |  |  |  |
| Enter explanation here | | | |

1. **Security Design/ Risk Assessment (RA) Activities[[18]](#footnote-18)**

**14.1 Describe security design/RA activities (check all that apply)**

|  | **Yes** | **No** | **Unknown** |
| --- | --- | --- | --- |
| Security Design Review (Please specify the security controls anticipated in being required to adequately protect the personal information) |  |  |  |
| Enter detail here | | | |
| RA completed (Please describe the risks determined to be in scope for this project as it relates to personal information) |  |  |  |
| Enter detail here | | | |
| Risk Mitigation Assessment completed (has there been a review of security controls and whether they will adequately mitigate the risks identified) |  |  |  |
| Enter detail here | | | |

**Reviewed by**

|  |  |  |
| --- | --- | --- |
| **Name and Title** | **Department/Faculty** | **Date** |
|  |  |  |
|  |  |  |

1. Data/Service Owner means any director, primary researcher or equivalent having authority and accountability for activities and records related to the data and the service provided. [↑](#footnote-ref-1)
2. Contact information should relate to individual most qualified to respond to questions about completed questionnaire. [↑](#footnote-ref-2)
3. In this context a project means the activity for which the privacy impact needs to be determined. This may include, but is not limited to, the development or acquisition of, or change to, a program, process, service, system, technology, application, or other project deliverable that will involve information or records. [↑](#footnote-ref-3)
4. For example, enterprise infrastructure or core services such as a technology platform or application, or a telecommunications product or service. Clients of the product or service will be responsible for the data that will populate the product or service. However, the project building or acquiring it needs to be mindful of whether or not personal information could be involved and of need of appropriate protection (e.g., if personal information will be involved then appropriate security measures must be adopted). [↑](#footnote-ref-4)
5. De-identify means to remove any information that explicitly identifies an individual, as well as any information that either alone or with other information could be used to identify an individual. [↑](#footnote-ref-5)
6. Data about an identifiable individual acting in their personal capacity. [↑](#footnote-ref-6)
7. A disclosure may be when personal information is transferred outside of an area or institution to another area or entity (e.g., another individual, another program area or organization). [↑](#footnote-ref-7)
8. A physical description or unique characteristic that identifies an individual may be considered personal information even without a name (e.g., a tall, one armed, blonde man who walks a brown poodle at the corner of Yonge and Bloor Streets every Wednesday at noon). [↑](#footnote-ref-8)
9. In limited circumstances, personal information may be excluded from the application of FIPPA under section 65 (e.g., some court records, labour relations and employment-related data, research and teaching material). Consult with the University Secretariat when determining if section 65 applies to the personal information related to your project. [↑](#footnote-ref-9)
10. The privacy provisions of FIPPA do not apply to personal information that is maintained as a public record. To qualify as a public record, personal information must meet a number of specific requirements. Consult with the University Secretariat when determining if section 37 applies to the personal information related to your project. [↑](#footnote-ref-10)
11. Direct collection is from the data subject, while indirect collection is from a third party. [↑](#footnote-ref-11)
12. The **Guidelines for the Protection of Information When Contracting for Services** provide guidance on how to address privacy in contracts with third party service providers. [↑](#footnote-ref-12)
13. Include organizations with any possible exposure or access to the personal information (e.g., developing, designing, building, testing, maintaining, storing or securing the data or systems resulting from your project). [↑](#footnote-ref-13)
14. The involvement of foreign organizations not subject to Canadian or Provincial privacy laws may pose a significant privacy risk. When personal information is stored outside of Canada or maintained in Ontario by a foreign-owned service provider or its Canadian affiliate, it could be subject to other countries' laws. Also, when contracting with a foreign-owned company, personal information about Ontarians or other sensitive information may be accessible to a foreign government. In addition, trade agreements may define requirements to be followed regarding management of information. Be aware of those that apply to your project. When in doubt, contact the University Secretariat or the Office of Legal Services. [↑](#footnote-ref-14)
15. The University Secretariat can help with the analysis of legislative and ministry-specific privacy issues. Consult the University Secretariat as early in your project lifecycle as possible. [↑](#footnote-ref-15)
16. The [Office of Legal Services](http://www.mcmaster.ca/ols/) can help with the analysis of statutory authority and application of privacy legislation. Consult with the [Office of Legal Services](http://www.mcmaster.ca/ols/) as early in your project lifecycle as possible, especially if your project is large scale, multi-department, cross-faculty, or involves contracting-out or alternative service delivery. [↑](#footnote-ref-16)
17. It is recommended for technology projects, that you consult with IT Security, [c-it-security@mcmaster.ca](mailto:c-it-security@mcmaster.ca), to assist with the identification of appropriate security controls and objectives to ensure that personal information is protected at collection and all the way through the lifecycle of data. [↑](#footnote-ref-17)
18. For assistance in performing a IT Risk Assessment please contact IT Security – UTS, [c-it-security@mcmaster.ca](mailto:c-it-security@mcmaster.ca) [↑](#footnote-ref-18)