WRDSB STUDENT CENSUS

Privacy Impact Assessment

STUDENTS COUNT, EACH AND EVERY ONE!

EXECUTIVE SUMMARY

The student census collects data specifically related to student identity, for the purposes of linking with identity-based data student outcome and student record data. The objective of this initiative is to support the board's efforts to identify and address systemic inequalities in our system. Student identity data to be collected includes Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and socio-economic characteristics. Identity data will be collected from parents for students from kindergarten to grade 3 and directly from students in grades 4 through 12+ (almost 65,000 students in total). The survey will be conducted electronically using the WRDSB's Qualtrics survey platform account. For parents/guardians that are unable to complete the census online, paper copies will be distributed and received by mail (this data will be entered into the Qualtrics platform by WRDSB research staff). Responses for each student will be attached to their student ID number and/or email address.

The student ID/email will be used to link individual student identity data to existing student record data including: student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation. An anonymized data set will be created using a key that assigns a unique (anonymous) identifier to each student. Once data has been linked, the student email/student ID number will be removed from the final data set and replaced with the anonymous unique identifier number. Only members of the research and IT department employees who require access for the purposes of data linking will be able to see the Student Census identity data in a form that is attached to a student's ID number or email.

The anonymized data set will be used for data analysis and will only be accessible to research department staff. A data suppression rule (15 students) will be applied to all documents and reports that are prepared for internal (school board) use and for the public.

A de-identified open data file will be released to the public free of charge, with appropriate privacy restrictions (e.g. suppression rule) applied prior to the release. The first public release will consist of reporting a full student profile, with the possibility of some school or board level comparisons across the system. The second phase of analysis and reporting will consist of linking student identity data with existing data kept on the student record/existing databases. Public reports and informational materials based on both student provided identity data and student record data will be released publicly and made available on the WRDSB website. Internal special interest reports will be developed for the purposes of informing policy and programming decisions, as well as supporting ongoing professional development initiatives.

The privacy impact assessment revealed that we have established protocols and/or procedures to address all major privacy issues with respect to this initiative. The Research Department will work with IT Services to ensure that long-term protocols are in place for the permanent disposal of personal information as per the WRDSB Records and Retention Schedule. The primary action item required subsequent to this assessment is a widespread communication and consultation strategy to ensure that the protocols outlined in this assessment are accessible to and understood by all affected parties (incl. students, parents, and staff).

Contents

INTRODUCTION

The WRDSB Student Census is a confidential and voluntary survey for all parents of WRDSB students from kindergarten and grade 3 and for all WRDSB students between grades 4 and 12. The goal of the student census is to better understand the diversity within the WRDSB. The census will allow us to gain detailed insight as to the cultural, social and demographic makeup of our students.

The Student Census will help us to develop a profile of all students that will allow us to better understand and address the needs of all students in the WRDSB regardless of their identity or their background. The findings will also help the board to better align our programs and strategies to the needs of all students and families in our school communities.

Identity-based student data collection is being undertaken by school boards across Ontario. The collection of identity-based student information is supported by and advocated for by the Ministry of Education's Equity Secretariat, Ontario's Anti-Racism Directorate, and the Ontario Human Rights Commission. As of 2018, the collection of identity-based student information is authorized under the Anti-Racism Act. By 2023, all Ontario School Boards will be legally required to apply the Data Standards for the Identification and Monitoring of Systemic Racism to collect identity-based student data.

The census will ask students and parents/guardians questions about the cultural, social, and sociodemographic identity of each student in the WRDSB. It specifically asks students and parents/guardians to report on their own or their child's Indigenous status, ethnic/cultural background, racial identity, first language, nationality, gender identity, sexual orientation, religious affiliation, health/disability status, socioeconomic characteristics, age, and grade.

The WRDSB Student Census is confidential and voluntary for all students. WRDSB adheres to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and applies a variety of best practice guidelines for the protection of students' personal information. No individual student data will be shared with anyone who does not need the information for the purposes of conducting research and preparing reports, unless required by law. By default, only members of the WRDSB research department will access to individual student responses (authorized members of the WRDSB Information Technology Services Department may require access to individual responses if necessary for technical support purposes). Reports prepared for WRDSB staff and for the public will never include information that will allow individual students to be identified.

Data security and privacy is important to the WRDSB. Student identity data from the Student Census will not be documented on their student record. However, student ID numbers and/or WRDSB student email address will be used to create a de-identified data file that will allow the WRDSB to compare and contrast student identity data with existing student data. Data that will be linked to the Student Census results include: student achievement, credit accumulation, suspensions/expulsions, special education services, and academic/extra-curricular program participation.

BACKGROUND

This privacy impact assessment is built on the groundwork of the privacy practices and protocols established for the WRDSB Workforce Census that was completed throughout 2019. This assessment found that our policies and procedures, when followed by all authorized employees, will protect student personal information and that it that meets and exceeds our legislative and regulatory commitments. Personal information is required to carry out this work (as per Ontario Regulation 267/18). Under the proposed procedures, all new personal information collected will remain confidential and will only be accessible in an identifiable format to a small number of authorized employees (specifically, research department staff and IT systems staff). We have identified three ways in which personally identifiable information could be viewed or accessed by unauthorized personnel:

1) if the release of the information is required by law (e.g. under an FOI request or in compliance with a criminal investigation)
2) unauthorized access to information occurs due to a failure of an authorized employee to follow the outlined security protocols
3) an unauthorized person engages in a sophisticated, surreptitious effort to gain access to personal information (for example hacking servers, or manipulating employees in a manner that would allow them to access private data)

An important part of this process will be an informed consent procedure that will provide parents and students with details of the purpose, process, privacy protocols, and opt-out procedures. All WRDSB Student Census processes adhere to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Scope: This privacy impact assessment includes only matters related to the collection of personal information through the Student Census survey and the processes used to link that information with existing identifiable student data held by the WRDSB. Any other research or data collection activity that might seek to make use of student identity data would be subject to a separate privacy assessment.

PROJECT

The student census collects data specifically related to student identity, for the purposes of linking with student outcomes and student record data. Student identity data to be collected include Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and community characteristics. Identity data will be collected from parents/guardians for students from kindergarten to grade 3 and each student between grades 4 and 12 (almost 65,000 students) electronically on the WRDSB Qualtrics survey platform account. For parents/guardians who are unable to complete the census online, paper copies of the census (with return envelopes included) will be mailed to their home. Responses for each student will be attached to their student ID number and/or email address.

The student ID/email will be used to link identity data for each to existing student record data including: student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation. An anonymized data set will be created using a key that assigns a unique (anonymous) identifier to each student. Once data has been linked, the student email/student ID number will be removed from the final data set and replaced with the anonymous unique identifier number. Only members of the research and IT department employees who require access for the purposes of data linking will be able to see the Student Census identity data in a form that is attached to a student's ID number or email.

The anonymized raw data set will be used for data cleaning and data analysis and will only be accessible to research department staff. A data suppression rule (15 students) will be applied to all documents and reports that are prepared for both internal (school board) and external (public) review.

A de-identified open data file will be released to the public free of charge, with appropriate privacy restrictions (e.g. suppression rule) applied prior to the release. The first public release will consist of reporting a full student profile, with the possibility of some school or board level comparisons across the system. The second phase of analysis and reporting will consist of linking student identity data with existing data kept on the student record/existing databases. Public reports and informational materials based on both student provided identity data and student record data will be released publicly and made available on the WRDSB website. Internal special interest reports will be developed for the purposes of informing policy and programming decisions, as well as supporting ongoing professional development initiatives.

PRIVACY

The personal information used in the Student Census process will be in two phases: Phase 1 - a student identity survey and Phase 2 – linking identity data to existing student outcome data. In the first phase of the project (Fall/Winter 2021), the student identity data that will be collected includes: Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and household characteristics. In the second phase of the project (Winter/Summer 2021), student ID/email identifiers will be used to link each student's responses to existing student record data including: student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation.

Legal Authority: The following Acts all authorize and regulate the proposed student census initiative:

- Education Act
- Municipal Freedom of Information and Protection of Privacy Act
- Personal Information Protection and Electronic Documents Act - *Model Code for the Protection of Personal Information*
- Anti-Racism Act - *Ontario Regulation 267/18, Data Standards for the Identification and Monitoring of Systemic Racism*
- Ontario Human Rights Code - *Ontario Human Rights Commission guideline – "Count me in! Collecting human rights-based data"*

In addition to these Acts, Ontario's Education Equity Action Plan is also a guiding document released in 2017 by the Ministry of Education that informed the processes and the priorities identified in this work.

Internal WRDSB Policies applicable to the Student Census include:

- Board Policy 1008: Equity and Inclusion
- Board Policy 1013: First Nation, Métis and Inuit Voluntary Self-Identification Policy
- Board Policy 1014: Privacy Protection and Access to Information
- Board Policy 2012: Access to Digital Resources and Technology
- Administrative Procedure 4070: Responsible Use Procedure for Information, Communication and Collaboration Technologies
- Administration Procedure 4770: Secure Disposition of Records

Access to all the guidelines, references and policies referenced above is available in the Appendix.

Roles and Responsibilities: The table below outlines key stakeholders in the census process and the high-level tasks and responsibilities associated with each stakeholder.

Stakeholder	Role/responsibility
Director of Education	Oversight and approval
Senior administration	Oversight and approval
Education Centre employees (incl. research, IT, privacy, equity, and communications)	Program management, including consultation, planning, communications, data collection, privacy, data management/ linking, data analysis, and reporting
School administrators	Process development and oversight of data collection at the school level.
Teachers, educational assistants, and student support workers	Facilitation of/oversight for data collection at the classroom level.
Parents	Participation in consultation, informed consent processes, voluntary completion of identity-based student census.
Students	Voluntary completion of identity-based student census.
Community-based groups[1]	Participation in consultation re. objectives and processes

Access to personal information:

Person	Access to all data	Can request individual data	Anonymous data file	Research reports
Student	No	Yes	Yes	Yes
Parent/guardian	No	Yes	Yes	Yes
WRDSB Research staff	Yes	Yes	Yes	Yes
WRDSB IT staff	As needed	No	Yes	Yes
School principals	No	No	Yes	Yes
Classroom teachers	No	No	Yes	Yes
Other WRDSB staff	No	No	Yes	Yes
The Ministry of Education	No	No	Yes	Yes
The general public	No	No	Yes	Yes

BUSINESS PROCESSES AND INFORMATION FLOWS

The Student Census does not represent a change in any normal business practices for collecting student data and conducting research for the purposes of improving programming and services available for students. However, given the sensitivity of collecting new personal information (identity-based data), it was determined that a privacy impact assessment was warranted. The privacy analysis presented below has been developed in alignment with the principles of the Canadian Standards Association's Model Code for the Protection of Personal Information, as referenced in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

[1] Equity and Indigenous Advisory Group, Waterloo Region Aboriginal Academic Advisory Committee, Waterloo Region Assembly of Public School Councils, Special Education Advisory Committee, Student Senate, and Parent Involvement Committee.

PRIVACY ANALYSIS

Privacy analysis: The Canadian Standards Association's Model Code for the Protection of Personal Information sets out ten principles for the protection of personal information. These principles were incorporated into the Personal Information Protection and Electronic Documents Act (PIPEDA), and they will be used as the foundation for this privacy analysis.

- **Principle 1 – Accountability**
  - The management of all personal information collected through the student census will be the responsibility of members of the Research and Evidence-based Practice Department (Dana Liebermann, Senior Manager, Research and Evidence-Based Practice). Guidance and support for the establishment and implementation of privacy protocols will be provided by the WRDSB Freedom of Information, Privacy and Records Information Management Officer, Sandra Vieira. Oversight for student census data that is linked to the student records will be coordinated between the Senior Manager of Research, Dana Liebermann and Senior Manager of Information and Technology Services, Ivana MacIsaac.

    Personal identifying information will never be shared with third parties under any circumstances unless required by law (such as when required for a criminal investigation, or to comply with a freedom of information request).

    Data privacy and security procedures will be developed and communicated publicly, including making this Privacy Impact Assessment available upon request. Contact information for Dana Liebermann, Sandra Vieira, and Ivana MacIsaac will be provided to all students, parents, and key stakeholders for the purposes of providing more information and/or to challenge compliance with applicable data privacy procedures and legislation. Multiple methods for contacting relevant WRDSB staff members (i.e. phone numbers and email addresses) will be communicated in notifications via email, letters home to parents, and on the board's public webpage.

- **Principle 2 – Identifying Purposes**
  - All communication to students and parents will include a description of why the student identity data will be collected and how it will be used. This will include communicating principles from relevant legislation, policies, and best practices. Communication will be distributed to all students and parents via email and letters sent home from schools. This will be conducted prior to the collection of data during the informed consent and student opt out phases of the student census process. The communication will include a commitment that the data collected will only be used for the purposes for which it was identified. If any changes are to be made to how personal data will be used, all affected parties will be informed of these changes and an opportunity to opt out of newly identified research activities will be provided prior to the proposed changes taking effect.

    The overarching objective of the student census is summarized in Ontario's Education Equity Action Plan as, "A consistent approach to collecting and analyzing voluntarily provided identity-based data will help local school boards identify where systemic barriers exist, and will help determine how to eliminate discriminatory biases in order to support equity and student achievement and well-being through training and targeted programs and supports." The WRDSB's approach is also consistent with the advice and guidelines established by the Ontario Human Rights Commission and the Ontario Anti-Racism Directorate.

The rationale for why identity-based data will be collected and how student outcome will be used will be communicated publicly. This will include the communication of specific questions that will be asked directly of students and parents/guardians, and a description of the student record data that will be linked to student identity data.

A summary list of identity data and student record data are provided below:

- Direct collection (student identity data): Indigenous status, ethnic/cultural background, racial identity, first language, nationality, gender identity, sexual orientation, religious affiliation, health/disability status, and community characteristics.
- Indirect collection (student record): credits accumulated, graduation status, special education services, suspensions and expulsions, refusal to admit a student, student achievement (i.e. EQAO/report cards), participation in academic program(s) (i.e. French immersion, International Baccalaureate, advanced placement), and participation in extra-curricular program(s) (i.e. student government, arts, athletics, volunteer placement programs).

Student record data will be disaggregated by student identity data for the purposes of identifying differences and gaps based on student identity.

- **Principle 3 – Consent**
  - The student census will use an active assent procedure for all student participants and an active consent procedure for parent/guardian participants. An informed opt out procedure will also be communicated to all parents of students under 18 years of age prior to the commencement of data collection.

    The active assent procedure will include oral and written communication to all students that the student census is voluntary and that they are able choose which questions they choose to answer and not to answer. They can choose not to begin the survey, they can skip any question in the survey that they do not wish to answer, and they can stop the survey at any time. Students will also be informed of the confidentiality procedures. This includes the fact that individual responses will not be shared with school or board staff (including their teacher and principal), and that they will be combined with the responses provided by other students in a way that will not allow them to be personally identified. Only research staff, and IT staff (on an as needed basis for technical support purposes), who require personal information for the purposes of conducting analysis and preparing reports will have access to identifiable data. The plain language informed consent statements will also include a description of how the information will be used, what information will be included in documents/reports, and how documents/reports will ensure that the personal information provided by students will remain confidential (including the use of password protected devices and folders, data suppression rules, and anonymous identifiers).

    Prior to starting the census questionnaire, students and parents/guardians will be asked if they agree to participate. This question stands as an assent questions for students and a consent question for parents/guardians. The assent/consent question is the only required question in the student census. The web-based survey will not proceed if a student or parent/guardian does not actively assent/consent to participate.

    Several communications strategies will be used to inform parents about the census and the opt-out procedures. An electronic (i.e. email, website, and social media) communications campaign will be implemented several weeks before the implementation of the student census. Parents will be able to communicate their desire

for their child (grade 4 and up, and under 18 years of age) to be exempt from participation in the census using an electronic or paper-based form. A link will be shared to direct parents to a web-based portal that will allow them to communicate their desire for their child to opt-out. Online instructions will also explain how they can express their preference by email or telephone for their child to be opted out of census participation.

A list of exempt students will be compiled and communicated to appropriate teachers and school administrators to ensure that the parents' desire for students not to complete the census is respected and enacted.

Contact information will also be provided to students and parents that will allow them to revoke their consent for the use of an individual students' identity data even after it has been collected. Once consent has been revoked, all personally identifying information provided by the student will be deleted, permanently and securely, from all data files and documents.

- **Principle 4 – Limiting Collection**
  - The WRDSB will only collect identity-based student data that has been legislated and/or recommended by Ontario's Anti-Racism Act and/or the Ministry of Education's Equity Secretariat. These include identities protected from discrimination under the Ontario Human Rights Code such as, race, ethnic origin, citizenship, creed, sexual orientation, gender identity, family status or disability.

    Data that is not required to meet our objectives for understanding differences among students based on these identities will not be collected from students.

    Data linking with student record data will not be indiscriminate. Specific data points from student records will be identified for data linking prior to data collection. Analysis will be primarily focused on disaggregating student results based on pre-identified student record data. Discretion will be used if additional data linking is undertaken. The same privacy and security protocols for data linking will apply to all supplemental data linking activities. If supplemental data linking deviates from the initial purpose and processes previously described to students and parents, a new description of the purpose and processes will be communicated to affected individuals and appropriate consent and opt-out procedures will be carried out.

- **Principle 5 – Limiting Use, Disclosure, and Retention**
  - Student identity data will be used only for the stated objective of identifying systemic differences and barriers and to determine how to support equity in student achievement and well-being. Student identity data will not be used or shared for any reason other than this purpose unless required by law (such as when required for a criminal investigation, or to comply with a freedom of information request).

    Only pre-authorized personnel from the Research and Evidence-Based Practice Department and the Information Technology Department will be granted access to voluntarily provided student identity data collected during the student census. All supplemental disclosure and communication of student identity data will be shared in an aggregated format that will not allow individual student identity data to be viewed by any unauthorized individuals. De-identified (aggregated) data files and reports will be prepared for internal and public release in accordance with Standard 35 of the Data Standards for the Identification and Monitoring of Systemic Racism under which the board is authorized (through the Anti-Racism Act) to collect student identity data.

These files will be made available in perpetuity, and the data in the files will support long-term assessment of change within our system.

Identifiable student identity data collected through the census will be kept for up to two years on password protected, encrypted external services (specifically our online Qualtrics survey platform). Student identity data collected during the student census will be transferred to password protected and encrypted WRDSB servers and will be securely disposed of in accordance with the WRDSB Records Retention Schedule. Student identity data kept on WRDSB servers will not merged or added to student records and will remain a distinct and confidential data set. The data will be used for longitudinal research to understand change in student demographics, student achievements, and student outcomes over time. Longitudinal research is consistent with the permitted used of personal information under the Education Act, specifically for the "Planning or delivering programs or services that the Ministry provides or funds, in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring and preventing fraud or any unauthorized receipt of services or benefits related to any of them."

All identity data will be deleted securely and permanently from all WRDSB servers in accordance with the WRDSB Records Retention Schedule.

- **Principle 6 – Accuracy**
  - The WRDSB will enact several data quality protocols to ensure the accuracy of the data provided during the student census. These protocols include:
    - Identifying and removing duplicate results
    - Using validity tests on datasets to identify illogical or incompatible responses (such as incongruous multiple choice selections from a single participant)
    - Reviewing reliability and consistency of census results compared to existing student records
    - Flagging inappropriate responses entered into open-ended text boxes

  Data quality protocols will be introduced at the beginning of the data collection period, such that appropriate corrective actions can be introduced as soon as possible.

  The collection and updating of student identity data will take place on a three to five year cycle and will be used to ensure new student data is captured to allow for further validation of existing student identity data.

  Personal identity data collection in the student census will not be used to make decisions about or develop interventions for individual students. Aggregated results will be used for program and system level decision-making and interventions, hence reducing risks that individual inaccuracies will have a substantive effect on decisions made and actions taken based on census results.

  Students and parents/legal guardians have a right to request access to view, and correct their personal information or the information of their child under the age of 18. Requests for access to data must be submitted in writing by a student and/or parent/legal guardian. Requests for access will be managed in accordance with MFIPPA. Under MFIPPA there are circumstances where data may not be released. All requests will be reviewed and a decision regarding the request will be communicated to the student and/or the parent/legal guardian.

- **Principle 7 – Safeguards**
  - Individual student identity data collected during the student census will never be printed or released in hard copy. Identifiable student identity data will remain exclusive on password protected and/or encrypted folders/devices. These locations include:
    - Qualtrics online survey platform. Cloud-based encrypted third-party servers (Canadian-based encrypted servers accessible only to WRDSB Research Department staff and to Qualtrics Inc. support staff when authorized by WRDSB Research Staff for technical support services)
    - Password protected WRDSB laptops of authorized personnel from the Research Department and the Information Technology Department
    - Password protected Google Drive folders (accessible only to authorized Research Department and Information Technology Department personnel).
  - WRDSB Research Department staff with the support of the Freedom of Information, Privacy & Records Information Management Officer conducted a Service Provider Privacy and Security Assessment on our online survey platform Qualtrics. The results of the assessment found that Qualtrics actively aligns their data security protocols with a number of international data security standards including: General Data Protection Regulation (EU), NIST SP 800-53 (US), FedRAMP (US), ISO 27001-2013 (international), and Privacy Shield (international). The assessment also confirmed that Qualtrics staff will not access data collected by the WRDSB without the permission of, or a request from, authorized WRDSB staff. WRDSB data collected using Qualtrics is stored at a secured data centre on encrypted third-party servers in Toronto, ON. Data on this server is accessible only to WRDSB Research Department staff and Qualtrics Inc. staff. Under normal business practice, Qualtrics staff will not access or share any of the survey data that is collected by the WRDSB without the expressed permission of authorized WRDSB employees.
  - To limit the risk that identifiable data will be seen or accessed, linked student census data and student record data will be kept in a separate, password protected folder and/or database distinct from both the student identity data on third-party server and data kept by the WRDSB on student records. Specific personal identifying information used for data linking (i.e. student ID and/or student email addresses) will be removed from the final working data set and replaced with an anonymous unique identifier number. A separate file will be prepared that aligns each student's anonymous identifier number to each student's student ID # and/or email address. Once a linked, validated and cleaned data file has been prepared with a unique anonymous identifier number for each student, any working data files used in the data linking process that include the student IDs and/or email addresses will be securely and permanently deleted. All data analysis will be conducted using a data set with anonymous identifiers. If necessary, Research and IT Department staff can use the anonymous ID and student ID alignment document to validate and/or correct an individual student's data in any files used for data analysis and reported.
  - Paper copies of the census received in the mail may only be opened and viewed by Research Department staff. Once opened responses will be entered into the online Qualtrics forms with the rest of student census data. Once opened, all paper copies of the census will be kept in a locked cabinet in the WRDSB Research Department accessible only to WRDSB staff. Once all data has been entered into the Qualtrics platform and data has been validated as accurate, the paper copies the census will be shredded and disposed of securely.

- In the unlikely instance of a data leak (or any breach of data privacy protocols), the exact nature of the data leak (or breach) and all corrective actions will be communicated to the Freedom of Information, Privacy, and Information Management Officer, and all affected parties as soon as possible.

- **Principle 8 – Openness**
  - Access to this privacy impact assessment will be made publicly available on the WRDSB website. Instructions for how to gain access to the document will be communicated as part of the informed consent phase of the process.

    Plain language summaries of data privacy and security protocols and procedures will be made publicly available, including links to relevant legislation and best practices. These documents will include general descriptions of applicable policies and regulations, informed consent procedures, and confidentiality/data security protocols.

    Contact information of relevant school board employees will be communicated to all parents and students as part of the communication and informed consent processes. They will include representation from the Peter Rubenschuh, Superintendent of the Human Rights and Equity Division, Dana Liebermann, Senior Manager of the Research and Evidence-Based Department, Sandra Vieira, Privacy and Records Information Management Officer, and Ivana MacIsaac, Senior Manager, Information Technology Services.

- **Principle 9 – Individual Access**
  - Students and parents/legal guardians have a right to request access to view, and correct their personal information or the information of their child under the age of 18. Requests for access to data must be submitted in writing by a student and/or parent/legal guardian. Requests for access will be managed in accordance with MFIPPA. Under MFIPPA there are circumstances where data may not be released. All requests will be reviewed and a decision regarding the request will be communicated to the student and/or the parent/legal guardian. For questions related to MFIPPA, students and parents/legal guardians may contact the WRDSB Privacy and Records Information Management Officer, Sandra Vieira, or Senior Manager of the Research and Evidence-Based Department, Dana Liebermann.

- **Principle 10 – Challenging Compliance**
  - Dana Liebermann, Senior Manager, Research and Evidence-Based Practice and Sandra Vieira, WRDSB Freedom of Information, Privacy & Records Information Management Officer, are responsible for ensuring WRDSB's compliance with relevant privacy legislation and the privacy and security protocols.

CONCLUSIONS

The WRDSB Student census is an important initiative that includes the use of personal and in some cases sensitive information. The protocols established to ensure the protection of privacy and to ensure data security are an integral part of giving participants confidence in our process, as well as adhering to our regulatory commitments.

Our protocols must be followed closely to ensure that our privacy and data security commitments are maintained. While it is impossible to ensure that a determined bad actor could never access private information to which they are not authorized, our protocols ensure that our processes and protocols meet best practices for preventing unauthorized access or residual identification through reporting. The most likely scenario by which personal information would be shared to an external stakeholder is through a legal, court ordered requirement. These could be issued under a Freedom of Information request or as required under a criminal investigation. In these instances, board employees will work to defend the privacy and confidentiality of student personal information as much as legally permitted.

This PIA has contributed to the establishment of protocols that, if followed closely, will limit the risk that any of the personal information collected from students could be used or accessed inappropriately or illegally. It is the responsibility of all staff participating in data collection, data management, and data analysis to follow the steps laid out in this assessment. The WRDSB will continue to assess and review its privacy and data management practices to ensure that we protect our students' rights to the privacy and security of their personal information.

NEXT STEPS

The processes and protocols herein will be communicated with all members of the Research Department and IT Services employees who will have access to identifiable student data from the Student Census. Research and IT Services staff are required to review and commit to the data security and privacy processes and protocols prior to accessing identifiable student data.

Research Department staff will collaborate with IT Services regarding safe disposal of data in accordance with the WRDSB Records Retention Schedule.

A copy of this PIA and other relevant information from the board will be available publicly on the board website.

APPROVAL

I, **the undersigned,** acknowledge that I understand the findings, privacy risks, and recommendations described this Privacy Impact Assessment and that I authorize implementation of the actions and mitigation strategies described herein.

Signature: 

Lila Read, Associate Director of Education
Waterloo Region District School Board

APPENDIX A: PRELIMINARY ANALYSIS QUESTIONNAIRE

1. PROJECT AND INSTITUTION

PROJECT TITLE	WRDSB Student Census
INSTITUTION	Waterloo Region District School Board
DEPARTMENT	Research and Evidence-based Practice Department
PROJECT LEAD	Dana Liebermann

2. PIA LEAD

NAME AND TITLE	Sandra Vieira
INSTITUTION	Waterloo Region District School Board
DEPARTMENT	FOI, Privacy & Records Information Management
PHONE NUMBER	519-570-0300, ext. 4409
E-MAIL	Sandra_vieira@wrdsb.ca

3. PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

In accordance with our board commitments to equity and inclusion, and under the authority of Ontario Regulation 267/18 (under the Anti-Racism Act, 2017) the Student Census will collect data specifically related to student identity, for the purposes of linking with student outcome and student record data. The objective of this work is to identify gaps and any evidence of systemic discrimination of students based on diverse student identities. Student identity data to be collected includes Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and socio-economic characteristics. Identity data will be collected from each student between grades 4 and 12 and from parents of children from kindergarten to grade 3 (almost 65,000 students). The student ID/email will be used to link each student's responses to existing student record data including: student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation. As per the Anti-Racism Data Standards, a de-identified open data file will be released to the public free of charge, with appropriate privacy restrictions applied prior to the release. Public reports and informational materials based on both student provided identity data and student record data will be released publicly and made available on the WRDSB website.

4. COLLECTION, USE AND DISCLOSURE

4.1 Identify the kinds of information involved in the project (check all that apply).

	YES	NO	UNKNOWN
Information about individuals in their personal capacity	✓		
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	✓		
Information about institutions, for example, for profit and not-for-profit institutions and government institutions		✓	
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	✓		

Note: as this pertains to students, the individual's 'official capacity' is that of a student.

An anonymized data set will be created using a key that assigns a unique (anonymous) identifier to each student. Once data has been linked, the student email/student ID number will be removed from the final data set and replaced with the anonymous unique identifier number. Only members of the research and IT department employees who require access for the purposes of data linking will be able to see the Student Census identity data in a form that is attached to a student's ID number or email. The anonymized raw data set will be used for data cleaning and data analysis and will only be accessible to research department staff. A data suppression rule (15 students) will be applied to all documents and reports that are prepared for both internal (school board) and external (public) review. A de-identified open data file will be released to the public free of charge, with appropriate privacy restrictions applied prior to the release. Public reports and informational materials based on both student provided identity data and student record data will be released publicly and made available on the WRDSB website.

4.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Student ID	✓	✓	✓		✓	
Student email	✓	✓	✓		✓	
Socio-demographic/cultural identifiers (Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and household characteristics) – *disclosure in anonymized format only*	✓	✓	✓	✓	✓	✓
	COLLECT	USE	RETAI	DISCLOSE	SECURE	DISPOSE
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.)						
Credit accumulation	✓	✓	✓	✓	✓	
Graduation rates	✓	✓	✓	✓	✓	
Special education services	✓	✓	✓	✓	✓	
Suspension and expulsion	✓	✓	✓	✓	✓	✓
Refusal to admit a student	✓	✓	✓	✓	✓	
Student achievement	✓	✓	✓	✓	✓	
Participation in academic program(s)	✓	✓	✓	✓	✓	
Participation in extra-curricular program(s)	✓	✓	✓	✓	✓	

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

All students registered with the WRDSB at the time of data collection (almost 65,000 in total).

5. PRIVACY LEGISLATION

5.1 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	✓		
None or other (Please explain below.)	✓		
Collection and use of student identity data is also regulated by the Education Act, the Ontario Human Rights Code and the Anti-Racism Act.			

5.2 Public Records and Excluded Personal Information

	YES	NO	UNKNOWN
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	✓		
The data will only be made available in a de-identified/aggregated format. The data will be made public in a machine-readable format (i.e. an Excel spreadsheet) as per the open data guidelines described in the Anti-Racism Data Standards. To prohibit the possibility of any subsequent or residual identification of individual students, suppression rules will be applied to all publicly available documents that are developed.			
Identify any personal information that will be excluded from the application of the acts by section 65 of *FIPPA* and section 52 of *MFIPPA*. What is the type of personal information and why is it excluded? (Please explain in row below.)		✓	

6. CONCLUSION

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.
We will proceed with the PIA as this process makes specific use of identifiable student data that is subject to regulations under MFIPPA, the Education Act, and the Anti-Racism Act.

APPENDIX B: PROJECT ANALYSIS QUESTIONNAIRE

1. SCOPE OF PIA

Define the scope of the PIA review and analysis, that is, what aspects of the project are in and out of scope.

The student census is focused on the collection, analysis, and reporting of student data. The only phases of this initiative that are out of scope for this initiative are aspects of the planning, consultation and communication protocols. However, the data security and privacy protocols will be integrated into these processes as well.

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

This work is currently authorized under the Anti-Racism Act [Ontario Regulation 267/18], the Education Act [Paragraph 8.1], MFIPPA (Part II - Protection of Individual Privacy - Collection and Retention of Personal Information), and the Ontario Human Rights Code [Paragraph 29(*c)*].

3. PROJECT CHARACTERISTICS

3.1 Identify key characteristics of the project (check all that apply).

	YES	NO	UNKNOWN
Involves creating a new program, process, service, technology, information system or other type of IT application	✓		
Involves a change to an existing program, process, service, technology, information system or other type of IT application	✓		
Involves procuring goods or services		✓	
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information		✓	

	YES	NO	UNKNOWN
Involves developing a request for bids, proposals or services		✓	
Involves a process, system or technology for which the privacy risks are not known or well documented		✓	
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	✓		
Involves information sharing (internal and external)	✓		
Involves the need to identify, authenticate or authorize users – public and/or internal staff	✓		
Other activities that may impact privacy. (Please explain below.)		✓	

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

The student census collects data specifically related to student identity, for the purposes of linking with student outcome and student record data. Student identity data to be collected includes Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and household characteristics. Identity data will be collected about each student from kindergarten to grade 12+ (approximately 65,000 students) electronically on the WRDSB Qualtrics survey platform account (paper collection available for those that require it). All student identity data will be attached to their student ID and email address. The student ID/email will be used to link identity data to existing student record data including student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation. An anonymized data set will be created using a key that assigns a unique (anonymous) identifier to each student. Once data has been linked, the student email/student ID number will be removed from the final data set and replaced with the anonymous unique identifier number. Only members of the research and IT department employees who require access for the purposes of data linking will be able to see the Student Census identity data in a form that is attached to a student's ID number or email. The anonymized raw data set will be used for data cleaning and data analysis and will only be accessible to research department staff. A data suppression rule (15 students) will be applied to all documents and reports that are prepared for both internal (school board) and external (public) review. A de-identified/anonymized open data file will be released to the public free of charge, with appropriate privacy restrictions applied prior to the release. Public reports and informational materials based on both student provided identity data and student record data will be released publicly and made available on the WRDSB website. Internal special interest reports will be developed for the purposes of informing policy and programming decisions, as well as supporting ongoing professional development initiatives.

3.3 Identify any changes that will result from the project (check all that apply).

	YES	NO	UNKNOWN
Involves a change in business owner		✓	
Involves a change to legislative authority		✓	
Involves a change in users (internal and external) of a related process or system		✓	
Involves a change in partners or service providers (internal and external)		✓	
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	✓		
Involves a change to the purposes for which personal information will be collected, used or disclosed	✓		
Involves a change from direct to indirect collection of personal information		✓	

	YES	NO	UNKNOWN
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information		✓	
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information		✓	
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software		✓	
Involves a change to an information system or database containing personal information		✓	
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients		✓	
Involves a change in the security requirements or measures		✓	
Other (Please specify change or proposed change below.)		✓	

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

The student census collects new (previously uncollected) data related to student identity, for the purposes of linking with student outcome and student record data. Student identity data to be collected includes Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and household characteristics.

The collection of this data is necessary to align with anti-racism legislation and to meet the board's commitment to collecting identity-based data for the purposes of identifying and responding to evidence of systemic discrimination in the Board.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

No additional businesses processes are required during any phase of the WRDSB Student Census.

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply)**.**

	YES	NO	UNKNOWN
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services		✓	
Involves logging information, usage or preferences, for example, IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology	✓		
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	✓		
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools		✓	
Involves processing or storing of personal information in a virtual environment, for example, cloud computing	✓		
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors		✓	

Involves developing, or customizing, software, hardware or IT support services “in-house”		✓	
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information		✓	
Involves a system or application that will automatically collect, use, disclose or retain personal information		✓	
Other (Please explain below.)		✓	

4.2 If you answered yes to any of the above, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

Our Third-Party survey platform (Qualtrics Inc.) tracks cookies as part of their regular business. The personal information collected during the Census will be stored in encrypted and/or password protected cloud-based servers accessible only to authorized personnel from the WRDSB or Qualtrics. Details on Qualtrics security protocols can be fully reviewed in our WRDSB Service Provider Privacy and Security Assessment of Qualtrics and our Student Census Privacy Summary (included as appendices to this PIA). These documents will be communicated publicly as part of our communication campaign.

De-identified, anonymized data files and reports will be prepared for internal and public release in accordance with Standard 35 of the Data Standards for the Identification and Monitoring of Systemic Racism under which the board is authorized (through the Ant-Racism Act) to collect student identity data. These files will be made available in perpetuity, and they will support the long-term assessment of change within our system.

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role.

INSTITUTION/THIRD PARTY	PROJECT ROLE
Qualtrics Inc.	Web-based survey provider. Technical support for the distribution of survey to student participants.

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information <u>on behalf</u> of your institution.

INSTITUTION/ THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE
Qualtrics Inc.	Web-based survey provider.	Hosts survey and facilitates third-party data storage of survey results. As regular business practice, does not access survey data unless requested or authorized by the client (in this case the WRDSB Research Department). More details are available in the WRDSB Service Provider Privacy and Security Assessment of Qualtrics

5.3 Identify any location outside of Ontario where personal information may be retained or stored and the third parties involved.

All personal information will remain within Ontario (including survey data on encrypted third-party servers).

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	RELATIONSHIP TO PROJECT	PROJECT ROLE
IT Services	Manages and has access to all locally hosted student data.	Has access to locally stored data (not Third-Party cloud storage) and may provide technical support in accessing and linking identity-based survey data and locally stored student data.

5.5 Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts	Qualtrics Inc.	✔		
Memoranda of Understanding				
Agreements (service level and trade)	.			
Other (Please explain below.)				

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed Project Analysis Questionnaire.

The following documents are accessible through links in Appendix D

- Board Policy 1008: Equity and Inclusion
- Board Policy 1013 – First Nation, Métis and Inuit Voluntary Self-Identification Policy
- Board Policy 1014: Privacy Protection and Access to Information
- Board Policy 2012: Access to Digital Resources and Technology
- Administrative Procedure 1102: Freedom of Information Request Protocol
- Administrative Procedure 1104: Privacy Breach Protocol
- Administrative Procedure 4070: Responsible Use Procedure for Information, Communication and Collaboration Technologies
- Administration Procedure 4770: Secure Disposition of Records
- WRDSB Service Provider Privacy and Security Assessment of Qualtrics
- Student Census Privacy Summary
- Qualtrics _ Security White Paper Lite 2018

7. PERSONAL INFORMATION FLOWS

7.1 Lifecycle of the personal information involved in the project

- In the spring of 2021, the student census collects data specifically related to student identity, for the purposes of linking with student outcome and student record data.
- Student identity data to be collected includes: Indigenous status, ethnic/cultural background, racial identity, first language, citizenship status, religious/spiritual affiliation, gender identity, sexual orientation, disability/health status, and household characteristics.
- Identity data will be collected from parents of children from kindergarten to grade 3 and directly from students between grades 4 and 12+ (approximately 65,000 students) using the WRDSB Qualtrics survey platform.

- Paper copies of the census will be sent to and received from parents/guardians who cannot be reached by emails. Paper copies of the census received in the mail may only be opened and viewed by members of the research department. The responses will be entered into the Qualtrics platform by research staff. Paper copies of the census will be kept in a locked cabinet in the research department, accessible only to members of the research department. Once entered into the Qualtrics platform data will be verified and validated. Research department staff will then shred and securely dispose of paper copies of census responses.
- Identity data for each student will be attached to each students' student ID and/or email address.
- The first phase of census reporting will not involve linking student identity data to existing student record data. Initial reports will develop board and school level profiles and some initial school and community demographic comparisons.
- An anonymized raw data set will be used for data cleaning and data analysis and will only be accessible to research department staff.
- A de-identified open data file will be released to the public free of charge, with appropriate privacy restrictions applied prior to the release.
- A data suppression rule (15 students) will be applied to all documents and reports that are prepared for both internal (school board) and external (public) review
- Public reports and informational materials based on both student provided identity data will be developed
- The second phase of data analysis and reporting will use student ID/email to link each student's responses to existing student record data including: student achievement, credit accumulation, graduation rate, suspensions/expulsions, special education services, and academic/extra-curricular program participation.
- An anonymized data set will be created using a key that assigns a unique (anonymous) identifier to each student. Once data has been linked, the student email/student ID number will be removed from the final data set and replaced with the anonymous unique identifier number. Only members of the research and IT department employees who require access for the purposes of data linking will be able to see the Student Census identity data in a form that is attached to a student's ID number or email.
- Reports generated from the second phase of data analysis will also be subject to the same de-identification, data suppression, and open data protocols as described for the first phase of analysis.
- Internal special interest reports will be developed for the purposes of informing policy and programming decisions, as well as supporting ongoing professional development initiatives.

APPENDIX C: PRIVACY ANALYSIS CHECKLIST

Answering the following questions can help you to identify the privacy risks that need to be addressed and the steps to be taken to ensure compliance with *FIPPA* or *MFIPPA*. You can use the table below to organize your work or it can be adapted to your own purposes and needs. Adapt to meet the needs of the project and your institution, while ensuring you address all the identified questions. Consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y[10]	N[11]	IP[12]	NA[13]	EXPLANATION		
Review each question and determine how each relates to the project. **Note:** Do not use the checklist as a substitute for the legislation. The statutory provisions have been summarized here.	Put a check mark (√) in the appropriate column for each question. This will create a visual representation of how the project will comply with *FIPPA* or *MFIPPA*. If your findings differ depending upon the type of personal information involved, add rows to document and explain the differences for each type.				Outline how you arrived at your findings. Provide as much information as is available, particularly if action is planned, but not yet implemented. Outline any options or alternatives that were, or need to be, considered. Explain why no action has been taken or planned for each "N" finding, and why requirements are "NA" to the project.	For each finding, outline the potential impact on privacy, for example, non-compliance with *FIPPA* or *MFIPPA*, increased intrusiveness into the private lives of individuals or it does not meet the public's expectation of privacy.	For each finding, identify the action(s) necessary for compliance with the privacy requirement or to mitigate or avoid a potential privacy impact.

10 **Y (Yes):** You know the privacy protection requirement either has been met by existing measures or will be met by action planned before implementation

11 **N (No):** You know nothing has been done or is planned to address this privacy protection requirement, that is, there is a possible privacy risk and "gap" in the project's compliance. If nothing has been done or planned, explain why.

12 **IP (In Progress):** You do not know the answer to the question at this time, that is, more information or analysis is required and, until such time, there is a potential privacy risk and gap.

13 **NA (Not Applicable):** You know this privacy protection requirement is not applicable to the project. Note: Be sure to check with your *FIPPA* or *MFIPPA* Coordinator and Legal Counsel.

A. COLLECTION

KEY REQUIREMENTS:

- For each collection of personal information, ensure that the institution collects personal information only if it has the authority to do so. Consider the following:
  - Is the collection expressly authorized by statute?
  - Will the personal information be used for law enforcement purposes?
  - Is the collection necessary for the proper administration of a lawfully authorized activity?
- Personal information should be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or statute.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- See sections 28 and 29 of *MFIPPA* and sections 38 and 39 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Is the collection of personal information authorized under *FIPPA* or *MFIPPA* or another act?	✓				Collection is authorized under MFIPPA, Ed. Act, and Anti-Racism Act (ARA).	Student personal information must remain secure.	Ensure that authorization is communicated publicly.
Do all parties collecting personal information have legal authority for the collection?	✓				Board employees are authorized as per legislation above.	Authorization for access needs to be restricted to research/technical staff.	Define/communicate data access authorizations.
Has responsibility for the collection been assigned to program staff or third party service providers?	✓				Research staff are managing data collection.	Allows for greater control off data flow and privacy.	Define/communicate data access authority publicly.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
PURPOSE OF COLLECTION							
Has the purpose of the collection been defined? What is the purpose of the collection?	✓				Collect student ID-based data to identify/eliminate systemic discrimination.	ID-based information needs to remain secure, access restricted.	Ensure that purpose and privacy is clearly communicated publicly.
NOTICE TO INDIVIDUAL							
Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.	✓				To be sent out via email, public website, and mail weeks before Feb 2020 data collection.	Important part of informed consent procedure.	Develop information and communications material for schools and parents.
Will the notice of collection comply with *FIPPA* or *MFIPPA*? Explain how or missing components.	✓				Notification, background info, and opt out procedures will be distributed widely.	Important part of informed consent procedure.	Develop information and communications material for schools and parents.
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the form of collection (for example, orally, hardcopy form, online portal, etc.)	✓				To be collected from students and parents/ guardians using Qualtrics survey platform (and paper through mail as needed).	Student and parent/ guardian emails will be used (by mail as needed). Data will be identifiable to WRDSB research staff.	Paper copies locked in cabinet accessible to researchers only. All data with identifiers are restricted to authorized staff.
Will personal information be collected indirectly from another source, or covertly? Why?		✓			Indirect from parents/guardians, young children unable to respond.	Indirect from parents/guardians requires additional communication.	Develop communication protocols for parents/guardians.
Will indirect collection comply with *FIPPA* or *MFIPPA*? Explain authority for indirect collection.	✓				Parent/legal guardian responding on behalf of their child.	Parents/guardians require additional communication.	Develop communication protocols for parents/guardians.
CONTROLS							
Will the project only collect personal information for which there is legal authority?	✓				Yes, as per MFIPPA, Ed. Act and ARA.	ID-based collection is authorized, but standards must be followed.	Continuous review of legislation/standards to affirm compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
Will there be periodic reviews of the collection controls to ensure effectiveness?	✓				Ongoing collaboration with WRDSB privacy officer.	Engagement with IT, school staff, and parents as needed.	Address stakeholder questions, apply/review privacy protocols throughout
DATA MINIMIZATION							
Is personal information necessary for the project to proceed?	✓				Needed to link with student record data to identify gaps.	ID-based data must be protected.	Restrict access to raw data files to researchers/IT staff.
Is collection of all the personal information necessary? Why or why not?	✓				The data collected aligns with ARD standards and Ministry recommendations.	Only collect necessary data.	Keep survey concise, focused on key (necessary) student sociodemographic info.

B. USE

KEY REQUIREMENTS:

- For each use of personal information, ensure that all parties involved in the project, for example, your institution, partners and other third parties, use personal information only with the authority to do so.
    - Is the use for the purpose it was collected or for a consistent purpose?[14]
    - Is the use authorized by the individual to whom it relates?
    - Does the use comply with another statute?
    - Is the use for other purposes permitted by *M/FIPPA*?
- See section 31 of *MFIPPA* and section 41 of *FIPPA*.

14 A consistent purpose is a use of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?	✓				Personal information will not be shared. Only de-identified data will be released.	Ensure access restrictions are clearly established to protect information.	Cite MFIPPA, Ed. Act, and ARA in communication materials.
PURPOSE(S) OF USE							
Has the purpose of the use been defined? Explain purpose(s).	✓				To identify/eliminate systemic discrimination.	To be communicated to students, parents, schools	Prepare communications materials.
Will personal information be used for other purposes?		✓			ID data will only be used for student equity research.	ID data will only be used for student equity	Communicate purpose and data use.
Will uses of personal information be for purposes stated in the notice of collection or for a consistent purpose?	✓				Purpose/resources will be communicated publicly. Not used for other purposes.	ID data will only be used for student equity research.	Communicate purpose and data use.
MANNER OF USE							
Have all parties using personal information been defined, for example, program staff, consultants, agents, third party service providers, etc.?	✓				Personal information will only be accessible to researchers and IT staff (as required).	Access to data will not be granted to unauthorized persons unless required by law (as per MFIPPA).	Communicate data access protocols during communication campaign.
CONTROLS							
Will there be procedural, technical, and physical measures in place to ensure personal information will be used only for authorized purposes and by authorized parties? Explain measures.	✓				Password protected and encrypted servers/folders. Locked physical documents. Open computers never to be left unattended.	Risk of inadvertent data leak.	Data privacy/protection protocols communicated to all staff with access to personal information.
Will there be periodic reviews of the use controls to ensure effectiveness?	✓				Review will be ongoing throughout project.	Protocols subject to change as needed.	Continuous reflection on access and reporting of data.
DATA MINIMIZATION							
Is use of all the personal information necessary for the project to proceed? Why or why not?	✓				Only necessary data will be collected to align to regulations.	Sensitive data must be safeguarded throughout process.	Review data collection protocols with stakeholders.

C. DISCLOSURE

KEY REQUIREMENTS:

- For each disclosure of personal information, ensure that all parties involved in the project, for example, your institution, partners and other third parties, disclose personal information only with the authority to do so. Consider the following:
  - Is the disclosure for the purpose for which it was collected or for a consistent purpose?[15]
  - Is the disclosure authorized by the individual to whom the personal information relates?
  - Does the disclosure comply with another statute?
  - Is the disclosure for other purposes permitted by *M/FIPPA*?
- See section 32 of *MFIPPA* and 42 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?	✔				Disclosure will be de-identified unless required by law (as per MFIPPA).	Confidentially builds confidence in process.	Keep data confidential, work with privacy officer if a legal request for data is made.
PURPOSE(S) OF DISCLOSURE							
Has the purpose of the disclosure been defined? Explain purpose(s).	✔				Disclosures to be explained to affected parties as per law.	Legal authorities responsible for privacy.	Comply with any legal requirements to disclose.
Will personal information be disclosed for other purposes?		✔			No disclosure unless legally required.	No disclosure unless legally required.	No disclosure unless legally required.

1 A consistent purpose is a disclosure of personal information that the individual to whom the personal information relates, that is, expect at the time of

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?	✓				Yes, board committed to confidentially. Will explain legal disclosure.	Unlikely to be required to release personal information.	Explain legal disclosure in during notice of collection/ informed consent.
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined, for example, program staff, consultants, agents, third party service providers, etc.?	✓				WRDSB (privacy, research, IT) commit to confidentiality, but will comply with legal obligation to disclose.	Unlikely to be required to release personal information, but legal possibility to be explained.	Explain legal disclosure in during notice of collection/ informed consent. Review with privacy officer.
Has the manner of disclosure been defined, for example, oral, mail, email, etc.?	✓				Nature of disclosure will be defined by the authority that required disclosure.	Nature of disclosure can't be defined ahead of time by WRDSB.	Commitment to communication with affected parties.
Will the disclosures be documented and how?	✓				Documented request/order is required as process.	Externally driven. No internally defined disclosures.	Document requests/ correspondence fully.
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?				✓	No information sharing agreements.	Personal information protected by WRDSB staff (research and IT).	No information sharing agreements.
CONTROLS							
Will there be controls in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain controls.	✓				Unauthorized parties will never have access to personal information (password protected, physically secured).	Risk for unauthorized, inadvertent access.	Authorized staff need to review data handling protocols.
Will there be periodic reviews of the disclosure controls to ensure effectiveness?	✓				Disclosures will be reviewed upon external legal requests.	Disclosure reviews undertaken if legally required.	Prioritize privacy and wellbeing of students before any disclosure.
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?		✓			No, we will not disclose information unless legally required to do so.	De-identification is the default approach. Suppression rules apply.	Communicate de-identification protocols and disclosure requirements.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[16]		✔			No, personal information disclosure is not needed for external research purposes.	Supplemental research would use de-identified data.	Prepare de-identified data files, as needed.
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[17]		✔			No, personal information will not be used for fundraising purposes.	Not an issue.	Reject any monetization of personal information.

D. ACCURACY AND CORRECTION

KEY REQUIREMENTS:

- Take reasonable steps to ensure personal information is not used or disclosed unless it is accurate, complete and up-to-date.
- Ensure that every individual is able to:
  - correct their personal information,
  - have a statement of disagreement attached to the personal information if the correction is not made and
  - require a notice of the correction or the statement of disagreement to be sent to anyone to whom the personal information was disclosed within the year before the above action was taken.
- See sections 30(2) and 36 of *MFIPPA* and 40(2) and 47 of *FIPPA*.

16 Before such a disclosure, there should be a defined and documented process that makes sure the researcher demonstrates why identifiable information is required for the research purpose, and agrees to the terms and conditions of Ontario Regulations 460 and 823, section 10.

17 *FIPPA* defines when disclosure of personal information by educational institutions or hospitals may be done for fundraising purposes. Before such disclosures, ensure the requirements, as defined in sections 42(2) and (3), have been met.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
STANDARD OF ACCURACY							
Will there be measures in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of measures.	✓				Quality assurance and data cleaning will be done before data analysis and reporting. Suspect data that can't be validated will be deleted.	During quality assurance and data cleaning data will be identifiable and extra security measures are needed.	Ensure that data is never left accessible in any format during quality assurance and data cleaning processes.
CORRECTING THE PERSONAL INFORMATION							
Will there be a defined and documented process for the processing of a request for the correction of personal information? Provide details of process.	✓				Parents/guardians and students must contact board in writing to discuss a request for the correction of personal information.	Requests will be reviewed on a case-by-case basis and will include communication with affected students and parents/guardians.	Received and respond to requests as received.
CORRECTION REQUESTS/STATEMENT OF DISAGREEMENT							
Will there be a defined and documented process for individuals to request the correction of their personal information? Provide details of process.	✓				Parents/students contact research department or privacy officer with request. Request reviewed and agreed action will follow.	Requests will be reviewed on a case-by-case basis and will include communication with affected students and parents/guardians.	Provide contact details for research and privacy officer data. Follow up on case-by-case basis.
CONTROLS							
Will controls be in place to ensure that only authorized personnel will be able to add, change or delete personal information?	✓				Unauthorized persons will have no access to identifiable student data.	Inadvertent access to be avoided by data security protocols.	Authorized employees work collaboratively to validate data.
Will there be periodic reviews of the controls to ensure effectiveness?	✓				Quality assurance ongoing. Case-by-case reviews.	Security and accuracy review an ongoing need.	Ongoing review of accuracy and security.

E. SECURITY

KEY REQUIREMENTS:

Take all reasonable measures to prevent unauthorized access to personal information in your custody or control, taking into account the nature of the record to be protected.

- Access should be restricted to only those individuals who need the personal information for the performance of their duties.
- Take all reasonable measures to protect personal information against loss or theft, unauthorized access, use or disclosure, inadvertent modification, destruction or damage, taking into account the format of the record to be protected.
- See Ontario Regulation 823, section 3 of *MFIPPA* and Ontario Regulation 460, sections 3 and 4 of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
SECURITY MEASURES							
Will measures be used to secure the personal information? Explain each physical, technical and procedural measure.	✓				Password protected and encrypted servers/folders. Locked documents. Data never left unattended.	Risk of Inadvertent access to data by unauthorized persons.	Data privacy/protection protocols communicated to all staff with access to personal information.
CONTROLS							
Will security policies and procedures be defined and documented to protect the confidentiality, integrity and availability of personal information?	✓				Privacy impact assessment will be made available for review. Will include protocols.	Ensuring awareness of and adherence to protocols by affected persons (accountability).	Fully communicating security protocols widely. Identify contact person to respond to questions.
Will testing and periodic reviews be conducted to ensure that personal information is only collected, accessed, used, disclosed, retained and disposed of when authorized?	✓				Protocols will be constantly reviewed with protection of personal information and best practices assessed throughout the project.	Making sure that affected persons can view and question protocols to ensure accountability.	Fully communicating security protocols widely. Identify contact person to respond to questions/issues.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?	✔				Protocols may be subject to review and update at any point in the project. Changes may be proactive or retroactive.	Proactive and responsive protocols implemented through communication and accountability.	Ongoing communication and consultation in all phases of the project.
Will procedures be defined and documented on how to identify, report, investigate and address the unauthorized access, collection, uses and/or disclosure of personal information?	✔				Privacy protocols communicated publicly, contact information to be communicated through schools, websites, and emails.	Ensuring that information for informed consent is accessible to all.	Use of multiple communications strategies to increase likelihood that information is available to all affected parties.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCESS REQUESTS							
Will the management of personal information change or restrict individuals' right of access to their personal information?		✔			Our processes are designed to adhere to MFIPPA legislation.	Confidentiality and student safety will be prioritized in all decisions and communication.	Provide contact information for privacy officer and research department.

G. RETENTION

KEY REQUIREMENTS:

- Personal information should be retained for at least one year after use to provide the individual with a reasonable opportunity to access their personal information.
- The individual's consent should be obtained in order to dispose of personal information prior to one year after use.

- Ensure compliance with other relevant records retention laws, regulations, bylaws or other requirements.
- See *MFIPPA* section 30(1) and Ontario Regulation 823, section 5; *FIPPA* section 40(1) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
RETENTION SCHEDULES							
Will there be defined and documented policies, procedures, and other requirements related to the retention of personal information?	✔				Data will be managed in accordance with the WRDSB Records and Retention Schedule.	Access and security of stored data is a long-term commitment.	Ensure that storage protocol is followed to support accountability.
REASONABLE OPPORTUNITY FOR ACCESS							
Will measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?	✔				Data will be managed in accordance with the WRDSB Records and Retention Schedule.	Access and security of stored data must be addressed long term.	Follow strategy to support accountability for data retention and deletion.
MEDIUM AND LOCATION OF RETENTION							
Has the medium and format of the personal information to be retained been defined?	✔				Input into Qualtrics, stored in distinct password protected files/databases.	Ensuring that authorized personal are aware of retention protocols.	Follow board retention protocols. Ensure adherence.
RETENTION PERIOD							
If the personal information has not been used, will it be retained for only as long as necessary to meet its purpose?			✔		The ongoing use of data is required for comparison over time.	The importance of maintaining security in subsequent, comparable WRDSB studies.	Storage protocols to ensure data can be accessed and revised for future use.
CONTROLS							
Will procedures be defined and documented related to consent for early disposal of personal information?	✔				No early disposal of data unless requested by an individual.	Data retention protocols need be clear as part of secure deletion process.	Communicate retention & deletion protocols to staff, students, and parents.
Will there be periodic reviews of the retention requirements and consent procedures to ensure effectiveness?	✔				Retention protocol may be updated if a compelling need is identified.	Notification may be required if a change is made.	Commit to notifying affected parties if policy changes.

KEY REQUIREMENTS:

- Personal information must be disposed by either securely destroying it or transferring it to the appropriate archives.
- Make sure personal information is only destroyed when authorized by an appropriate party and in accordance with records retention regulations/bylaws applicable to the institution.
- Take all reasonable steps to protect the security and confidentiality of personal information to be destroyed throughout the process, that is, when personal information is stored, transported, handled and destroyed.
- Take all reasonable steps to protect the security and confidentiality of personal information to be transported to archives throughout the process, that is, when personal information is stored, transported and handled.
- Take all reasonable steps to destroy personal information so it cannot be reconstructed or retrieved.
- Keep an accurate record of the disposal, including what personal information was destroyed or transferred and on what date it was destroyed or transferred.
- Do not include personal information in your record of disposal.
- See Ontario Regulation 823 and section 30(4) of *MFIPPA*, section 3 of *MFIPPA* and Ontario Regulation 459 and section 40(4) of *FIPPA*.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
MANNER OF DISPOSAL							
Will procedures be defined and documented for the secure disposal, for example, transfer to archives or destruction of personal information in accordance with applicable records retention schedules, regulations/ bylaws? Explain disposal process.			✔		Research to establish understanding with IT services and third party survey platform to ensure data is securely & permanently deleted.	Ensuring that residual access to data is never allowed, via data that was not securely removed from servers or devices.	Review and apply best practices for secure destruction of data once the retention periods have ended.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS				EXPLANATION	PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA			
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?			✓		Protocols for secure disposal of data and devices to be confirmed with IT.	Ensuring that residual access to data is never allowed.	Review secure data and device destruction protocols with IT services.
CONTROLS							
Will controls be defined and documented to ensure only appropriate personal information will be disposed of or destroyed, and only by authorized parties after obtaining appropriate approval?	✓				Research staff will ensure third party survey secure disposal. IT services will ensure secure disposal of data on WRDSB servers and devices.	Protocols and processes to align with board retention schedule and secure disposition of records policies.	Follow up with IT to ensure secure data deletion and device destruction as per board procedures.
Will there be periodic reviews of the disposal controls to ensure effectiveness?			✓		Procedures will align with emergent best practices and regulations.	Research data disposal and IT practices needed to protect personal info.	Follow protocol with IT to ensure secure/permanent data disposal protocol.
RECORD-KEEPING							
Will details of the disposal of personal information be recorded?			✓		Retention/disposal practices communicated.	Avoid risk of residual release of personal info.	Include retention/disposal practices in comms material
Will measures be defined and documented to ensure no personal information is captured in the disposition record?	✓				Best practices to ensure secure and permanent disposal of data will be used.	Protocols must ensure that personal info is never accessed by unauthorized persons.	Follow board protocols with IT.

I. PRIVACY MANAGEMENT

The questions in this section relate to privacy management throughout your institution. They are not limited to the project's information system, technology or program, but address your institution's privacy maturity, capability and readiness to undertake the project. The emphasis is on accountability and training.

KEY REQUIREMENTS:

- You should apply common management principles, for example, planning, directing, controlling and evaluating the personal information collected, used, disclosed, retained and destroyed by institutions.

  Establish and follow disciplined and consistent practices for the management of personal information.

  Educate staff about privacy, as well as legislative and other relevant requirements.

- Periodically review privacy policies and practices, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCOUNTABILITY							
Will accountability for managing personal information throughout its lifecycle be defined to include parties involved in the project, for example, your institution, partners, vendors and other third parties? Explain accountability.	✓				Accountability for managing info will be responsibility of research and IT. Privacy officer will provide advice and oversight as needed.	If protocols are not followed, risks of unauthorized access and use increase. Management personnel must remain committed to privacy/security protocols.	Communicate protocols clearly to all responsible managers (research, IT, and privacy).
TRAINING							
Will operational policies, procedures or practices related to the protection of personal information be needed?	✓				Yes, these practices are in place.	Policies/practices are needed to ensure data is protected.	Ensure awareness of policies and practices.
Have all parties requiring training on operational, security and privacy aspects of the project been identified?				✓	No new training required.	Authorized staff are aware of responsibilities/practices.	Ensure ongoing communication.
Has the individual responsible for ensuring that all parties receive appropriate training been identified?				✓	No new training required.	NA	NA
AUDITS							
Will procedures and protocols be developed and documented to evaluate whether the personal information is accessed, collected, used, retained, disclosed, secured and disposed of in a manner that is consistent with *FIPPA* or *MFIPPA*?	✓				All protocols will be posted publicly and contact information for questions and concerns will be widely distributed.	Transparency is an important part of accountability and informed consent.	Communicate data privacy practices and protocols broadly and publicly.

APPENDIX D: SUPPLEMENTARY DOCUMENTS

Legislation:

- Education Act: https://www.ontario.ca/laws/statute/90e02
- Municipal Freedom of Information and Protection of Privacy Act: https://www.ontario.ca/laws/statute/90m56
- Personal Information Protection and Electronic Documents Act: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
- Anti-Racism Act: https://www.ontario.ca/laws/statute/17a15
    - Ontario Regulation 267/18: https://www.ontario.ca/laws/regulation/r18267
- Ontario Human Rights Code: https://www.ontario.ca/laws/statute/90h19

Best Practice Guidelines:

- Model Code for the Protection of Personal Information: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html
- Anti-Racism Data Standards: https://www.ontario.ca/document/data-standards-identification-and-monitoring-systemic-racism
- Ontario Human Rights Commission guideline – "Count me in! Collecting human rights-based data": http://www.ohrc.on.ca/en/count-me-collecting-human-rights-based-data
- Ontario Student Record (OSR) Guideline, 2000: http://www.edu.gov.on.ca/eng/document/curricul/osr/osr.html

Internal WRDSB Policies and Administrative Procedures applicable to the Student Census include:

- Board Policy 1008: Equity and Inclusion: https://www.wrdsb.ca/wp-content/uploads/1008-Equity-and-Inclusion.pdf
- Board Policy 1013 – First Nation, Métis and Inuit Voluntary Self-Identification Policy: https://www.wrdsb.ca/wp-content/uploads/1013-FNMI-Voluntary-Self-Identification.pdf
- Board Policy 1014: Privacy Protection and Access to Information: https://www.wrdsb.ca/wp-content/uploads/1014-Privacy-Protection-and-Access-to-Information.pdf
- Board Policy 2012: Access to Digital Resources and Technology: https://www.wrdsb.ca/wp-content/uploads/2012-Access-to-Digital-Resources-and-Technology.pdf
- Administrative Procedure 1102: Freedom of Information Request Protocol: https://www.wrdsb.ca/wp-content/uploads/1102-FOI-Request-Protocol.pdf
- Administrative Procedure 1104: Privacy Breach Protocol: https://www.wrdsb.ca/wp-content/uploads/1104-Privacy-Breach-Protocol.pdf
- Administrative Procedure 4070: Responsible Use Procedure for Information, Communication and Collaboration Technologies: https://www.wrdsb.ca/wp-content/uploads/AP4070-Responsible-Use-Procedure-for-Info-Comms-and-Tech.pdf
- Administration Procedure 4770: Secure Disposition of Records: https://www.wrdsb.ca/wp-content/uploads/AP4770-Secure-Disposition-of-Records.pdf

Communication and informational documents shared publicly:

- WRDSB Service Provider Privacy and Security Assessment of Qualtrics

WRDSB Service Provider Privacy and

- Qualtrics - Security White Paper Lite – 2018

Qualtrics _ Security White Paper Lite 201