Service Provider Privacy and Security Assessment Tool

This questionnaire must be completed by all organizations that provide services to the school board that involve the collection, access, disclosure and retention of student and/or staff personal information.

Name of Service Provider (the "Organization"): Qualtrics International Inc.

Service Provided or Role of the Organization: Web-based survey and data analysis software

Describe the types of Personal Information ("Data") to be collected by or disclosed to the Organization:

- It is up to WRDSB to determine the type of data collected by the platform. Below is a summary of the type of data that is normally collected.

  TYPES OF DATA COLLECTED
  There are several data types that surveys collect, and each type generally falls into one of the following categories:
  - **Response Data:** Data that survey respondents provide by answering questions in surveys or employee evaluations.
  - **Panel Data:** A panel is a respondent list that the Brand can use for the distribution of surveys. This usually includes email addresses paired with a name, but can include additional information. Use of panels is optional.
  - **User Information:** The requisite username (User login ID) and password for logging into the platform. All logins are logged, and the Qualtrics User can easily view the log. Usernames are chosen by the Brand Administrator, must be unique for the entire Qualtrics platform, and need not be an email address.
  - **Survey Design and Objects:** Surveys created by a Customer along with any graphics and other property uploaded by a Customer and hosted by Qualtrics for use in surveys. Graphics and other objects may be stored in a library.

  Qualtrics does not represent or attest to Data entered into its Services since all Data is controlled by the Customer in a self-service, one-to-many business model.

ACCOUNTABILITY AND POLICIES

1. Who is responsible for privacy compliance within your organization?

- "A detailed incident response policy is maintained by the InfoSec and Legal departments… Qualtrics has developed Incident Response policies and procedures to ensure the integrity, confidentiality, and availability of the Data. These policies and procedures are consistent with applicable federal laws, Executive Orders, directives, regulations, standards, and guidance and are set forth by the management teams in compliance with the Incident Response family of controls found in NIST SP 800-53." - *Qualtrics Security White Paper (p. 12)*

2. Who is responsible for information security within your organization?

- "Qualtrics has suitable policies to handle these requests, and has a team of outside attorneys, privacy staff, and security experts to respond to the particular notification needs based on the content disclosed." - *Qualtrics Security White Paper (p. 12)*

3. Is your organization compliant with the European Union General Data Protection Regulation? If not, why not?

- Qualtrics has specifically included features that allow all its customers to meet the requirements of the GDPR: *'Safe. Secure. And ready for GDPR'* - https://www.qualtrics.com/uk/platform/gdpr/. It features functions that ensure that users can secure, correct, and protect any personal data that is collected. *Note: it is the responsibility of the WRDSB to manage their data and their usage of the platform to ensure this alignment, as Qualtrics does not access or manage the data collected by customers without the consent of its customers.*

4. Please provide a copy of your privacy policy and related procedures or documents providing guidance for staff regarding the appropriate use and safeguarding of personal information.

- See below links for Qualtrics documents with security and privacy policies and practices:
    - Privacy statement: https://www.qualtrics.com/privacy-statement/
    - Qualtrics Security White Paper Lite (see attached document)
    - Terms of Service: https://www.qualtrics.com/terms-of-service/

5. Do all of your employees commit in writing to follow confidentiality and security standards for handling customer/personal information, e.g. non-disclosure/confidentiality agreements?

- EMPLOYEE AGREEMENTS - Upon hire, all Qualtrics employees are required to sign a privacy and confidentiality agreement that specifically addresses the risks of dealing with confidential information, including Customer accounts and Data. The policy includes the prohibition of access to Data without User permission—typically granted for technical support only.

6. Does the organization have a disaster recovery plan?

- "Qualtrics provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed." – *Privacy Statement – Section 5.* Also see *Security White Paper -> Business continuity & disaster recovery* (p. 6) for more detail.

7. Has a privacy assessment, audit and/or security review been performed on your organization in the past? How often are these conducted? By whom? What qualifications are held by the assessor/auditor? Please provide available results or information from such assessments, audits or reviews.

- Qualtrics is FedRAMP authorized and ISO 27001-2013 certified. Qualtrics also self-certifies with Privacy Shield (https://www.privacyshield.gov/welcome). Self-assessment is signed by a company officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance. - *Privacy Statement – Sections 3 and 5*

8. Do you include a "right to audit" clause in your contracts?

- "Under Privacy Shield, an individual has the right, under certain conditions, to invoke binding arbitration for complaints regarding Privacy Shield compliance not resolved by any of the other Privacy Shield mechanisms. Under Privacy Shield, Qualtrics must respond to individual complaints within 45 days." *Privacy Statement – Section 5*

9. Does your organization regularly obtain a SSAE 16 (U.S.) or CSAE 3416 (Canadian) Service Organizational Report to provide customers with the assurance your organization is maintaining effective and efficient internal controls related to financial, informational or security reporting?

- Our production Services are hosted by third-party data centers that are audited using industry best practices (including SOC reports). The infrastructure is located in dedicated space that is physically separate from other data center tenants. The third party provides physical and environmental controls, but Qualtrics owns and operates all of the physical infrastructure. The data center provider does not have logical access to Qualtrics infrastructure.

10. How frequently does your organization review and update information handling practices and related documentation?

- Annually

11. Do plans exist to identify security breaches or inappropriate disclosures of personal information that occur within your organization? What tools are used for this purpose?

- INCIDENT[1] RESPONSE PLAN - Qualtrics has developed Incident Response policies and procedures to ensure the integrity, confidentiality, and availability of the Data. These policies and procedures are consistent with applicable federal laws, Executive Orders, directives, regulations, standards, and guidance and are set forth by the management teams in compliance with the Incident Response family of controls found in NIST SP 800-53. An Incident includes:
    - A malfunction, disruption, or unlawful use of the Service;
    - The loss or theft of Data from the Service;
    - Unauthorized access to Data, information storage, or a computer system; or
    - Material delays or the inability to use the Service
    - Any event that triggers privacy notification rules, even if such an event is not due to Qualtrics' actions or inactions
- DATA BREACH NOTIFICATION REQUIREMENTS - An Incident involving personal data (as defined by applicable regulations or laws) may require certain notification procedures. Qualtrics has suitable policies to handle these requests, and has a team of outside attorneys, privacy staff, and security experts to respond to the particular notification needs based on the content disclosed.

INFORMATION FLOW

1. Is the school board data you collect retained in paper format, electronic format or both?

- WRDSB owns all the data it collects (*Terms of Service – Section 4.1*) and stored electronically in encrypted third party data centres.

[1] An incident in this section refers to any discovery of deliberate or accidental mishandling of Data (collectively, an "Incident"). A detailed incident response policy is maintained by the InfoSec and Legal departments.

2. Where will the data obtained from the school board be stored at your organization?

- Canadian third party data centre in Toronto and AWS Canada.[2]

3. Is the school board data processed or stored outside of Canada? If so, where and how?

- "Unless required by law, Qualtrics will never transfer Data to a third party without the written permission of the customer" - *Privacy Statement – Sections 3*.
- During the normal provisioning of the Qualtrics services, no data are transferred between geographical regions." - *Privacy Statement – Sections 3*.

4. How do you ensure that school board data is kept secure and separate from the data of other organizations?

- DATA STORAGE - Qualtrics Services use databases that logically store Data, as well as organize other components for quick retrieval and faster processing. All hardware and software are shared among Customers.

  Access to Data requires direct ownership (the user who created the survey) or implied access (e.g. Brand Administrator or another User with access). Response Data is separated by logical controls using the Brand ID as an identifier and verifier. Thus, during each read request, response Data is verified by the ID to ensure accuracy.

5. Does your software collect cookies? If so, for what purpose?

- Qualtrics uses cookies during website visits to www.qualtrics.com in efforts to customize content to the needs of customers (No personal data are collected when browsing this site.) – *Privacy Statement – Section 2.* See *https://www.qualtrics.com/support/survey-platform/getting-started/browser-cookies/* for more details.

6. Is school board data ever used for purposes unrelated to the services being provided to the school board?

- Qualtrics does not directly access or use the personal data collected by WRDSB (except for anonymized software usage data). The Qualtrics Brand Administrator has full access to the board user accounts, but does not access board data unless requested by authorized board staff or required for legal or a legitimate business need. - *Qualtrics Security White Paper - p. 11 and 17*

7. Is school board data ever merged or matched with data that has not been provided by the school board? If so, please explain.

- See response to previous question

8. Is school board data ever provided to a service provider of your organization, a contractor, or any other third party outside of the organization? If so, specify the third parties and the purposes for the sharing school board data with them. What steps have been taken to ensure that school board data remains safeguarded?

[2] Amazon Web Services Canada: https://aws.amazon.com/canada/aws-in-canada/

- "Unless required by law, Qualtrics will never transfer Data to a third party without the written permission of the customer. In other words, there is no onward transfer." - *Privacy Statement – Section 3*
- "All access to Qualtrics front-end Services is via Hypertext Transfer Protocol Secure (HTTPS) and enforces HTTP Strict Transport Security (HSTS). The platform supports Transport Layer Security (TLS) for all interaction with the platform. Access to the back-end services using the Qualtrics API supports TLS v1.2. Data is processed by application servers and sent to database servers for storage." – *Qualtrics Security White Paper - p. 9*
- "Qualtrics backs up all customer data each night, and retains the backup dataset for 90 days. After 90 days, the backup dataset is deleted."– *Safe. Secure. And ready for GDPR - FAQ – 'Is personal data permanently deleted when I remove it?'*

9. Is school board data transmitted over secure channels and/or encrypted?

- See response to question 8

10. How long is school board data retained by your organization? Can you accommodate applying retention periods as directed by the school board? Specify the current retention period your organization implements for data stored in both electronic and paper format.

- Customers determine the following about the data stored in the Qualtrics platform:
    - Which type of data to collect
    - Who to collect data from
    - Where to collect data
    - What purpose
    - When to delete the data
- Qualtrics recommends that customers "… ensure that all contacts and personal data are deleted prior to terminating Your Qualtrics brand, especially if required by policy, law, or regulation." - *Safe. Secure. And ready for GDPR - FAQ – 'How long is personal data retained in Qualtrics if I don't delete it?'*
- At the end of a customer contract, accounts are left active for 30 days after the contract ends to allow customers to delete the data from the platform. Afterwards, the data resides in our backups for 90 days before it is permanently deleted.
- WRDSB has full access to be able to permanently delete data at any time:
    - "Qualtrics philosophy is that customers own and control all the data they collect." - *Safe. Secure. And ready for GDPR - FAQ – 'How long is personal data retained in Qualtrics if I don't delete it?'*
    - "A deleted response is initially flagged for deletion, and may be recovered by Qualtrics Support (Quni) upon requested. After 90 days, the deletion becomes permanent and unrecoverable." – *Safe. Secure. And ready for GDPR - FAQ – 'Is personal data permanently deleted when I remove it?'*
    - "To permanently and immediately delete data, the Brand Administrator (or a user with equivalent permissions) may perform a permanent deletion. Permanently deleted data are

unrecoverable, even by Qualtrics Support." – *Safe. Secure. And ready for GDPR - FAQ – 'Is personal data permanently deleted when I remove it?'*

11. If the data is being destroyed or returned to the school board, how is this done and how is it documented?

- Encrypted data is deleted and destroyed when authorized by WRDSB staff
    - "To permanently and immediately delete data, the Brand Administrator (or a user with equivalent permissions) may perform a permanent deletion. Permanently deleted data are unrecoverable, even by Qualtrics Support." – *Safe. Secure. And ready for GDPR - FAQ – 'Is personal data permanently deleted when I remove it?'*
- The Board owns the data, so Qualtrics does not need to 'return' the data as it is encrypted at the third party data centre (see references above). The data can be deleted by the Board at any time. Data that is not deleted by the Board at the end of a contract is permanently deleted from encrypted servers 90 days following the conclusion of the contract.

SAFEGUARDS

1. Who within the organization has access to school board data? Specify access rights by role type (e.g. full/partial to all/specific types of data), and the service each role provides that deems access necessary.

- "Access to Customer accounts is only given to those with a legitimate business need and with explicit approval. This includes members of the Qualtrics support teams (QUni and Client Success), engineering team for specific debugging issues, and select members of our onboarding team that handle creating accounts for new customers. All system and service logins are logged. No employee has unfettered access to Customer Data." - *Qualtrics Security White Paper - p. 11*
- "Qualtrics treats all Data as highly confidential and does not classify or represent the Data because only the Customer itself knows what data it's collecting. In other words, Qualtrics provides the services, and Customers use the services as they wish. All Data are safeguarded using industry best security practices that prevent unlawful disclosure." - *Privacy Statement – Section 3*

2. Who in your organization is responsible for overseeing privacy/security protections? What are their qualifications?

- The Legal Department is responsible for privacy within Qualtrics. Information Security is managed by the Information Security team. Each team is made up of accredited professionals.

3. Can access to and changes to school board data by your employees be audited by date and user identification?

- Various tools are used to monitor the confidentiality, integrity, availability, and performance of the production environment, such as intrusion detection systems, performance and health systems, and security event correlation systems.
- SECURITY MONITORING - The platform is monitored for security breaches, system performance, and other key performance indicators. Service teams have configured production servers, databases, and network devices to report their logs into a Security Information and Event

Management (SIEM) system. The production systems are configured to capture log events including: logon events, account management events, privilege functions, and other system events. The SIEM is configured to monitor and alert when certain thresholds and activities are performed.

Alert notifications are monitored by the Security Operations Center (SOC) and service teams. Alerts are acknowledged and corrective action is taken as needed. Documented procedures are followed to address security breaches, incidents, and service disruptions. Automated monitoring systems are supplemented with manual reviews of system logs and physical access logs.

4. When and how is your employee access to school board data revoked?

- As soon as specific access to systems/services/software is no longer required for job responsibilities, it is revoked. This includes termination of employment as well as changes to roles or responsibilities in the company. The uncoupling process is completed within 24 hours of a role change, or immediately at employment termination. During such an event, a ticket gets created by a manager or HR employee, and emails get sent to various departments. The ticket is managed by HR to ensure that all actions are being performed during the change/termination (such as access to systems and buildings).
- All the terms related to accessing board data must be prepared and approved by authorized WRDSB staff

5. Can school board data be accessed remotely by your employees? If so, what safeguards are in place for that remote access?

- ACCESS AUTHENTICATION - Access to the production environment is managed through multiple network and authentication layers using multiple usernames, passwords, and multi-factor authentication (MFA) tokens. Prior to accessing the production environment, access to a specific corporate network is required. Access to that network is managed via a username, password, and MFA token. Once connected to the correct corporate network a separate username, password, and MFA key is required to access the production environment through a bastion host. Once connected to the bastion host, an administrator is able to connect to the target system.

  Access to our public cloud infrastructure (AWS) requires a username, password, and MFA token to access the management console.

  Access to the production infrastructure is restricted to authorized personnel based on job function. Privileged system access is restricted to a limited number of system administrators and their management.

6. Do you maintain a close inventory of your computers?

- Physical inventories of all production systems are documented and maintained for tracking and reporting purposes. A physical inventory of production systems is performed periodically.

7. What technical and physical safeguards are in place to ensure that school board data is protected from loss, theft, unauthorized access, or inadvertent disclosure?

- DATA STORAGE - Qualtrics Services use databases that logically store Data, as well as organize other components for quick retrieval and faster processing. All hardware and software are shared among Customers.

  Access to Data requires direct ownership (the user who created the survey) or implied access (e.g. Brand Administrator or another User with access). Response Data is separated by logical controls using the Brand ID as an identifier and verifier. Thus, during each read request, response Data is verified by the ID to ensure accuracy.

  All Data is stored within the region where the Customer's primary data center resides, and will not be moved from that region. In other words, if a European customer has its data collected in the EU, its data will be stored and processed in EU. Qualtrics does not transfer Data unless requested by the Customer.

- ENCRYPTION OF DATA IN TRANSIT - All access to Qualtrics front-end Services is via Hypertext Transfer Protocol Secure (HTTPS) and enforces HTTP Strict Transport Security (HSTS). The platform supports Transport Layer Security (TLS) for all interaction with the platform. Access to the back-end services using the Qualtrics API supports TLS v1.2. Data is processed by application servers and sent to database servers for storage. Respondent Data includes survey questions, graphics, and other content created in the survey design.

8. Does your organization maintain secure backups of school board data? How is this done?

- BACKUP CONFIGURATION - Qualtrics performs a full backup twice a week and daily incremental backups of all production data. These backups are stored at alternate data centers in the same region where the data were created. Production backup files are encrypted using Advanced Encryption Standard (AES)-256.

9. Is all school board data erased when disposing of computer hardware/software? How is this done?

- Formal processes and procedures are in place to securely dispose of devices that may contain Customer Data. These procedures apply to all data center environments. Deprecated or defective media (specifically, hard drives) are erased according to a U.S. Department of Defense compliant 3-pass overwrite standard, and/or physically destroyed.

10. What methods are used to control and monitor physical access to your organization's premises?

SITE OPERATIONS - Qualtrics is responsible for the physical security controls at the Corporate offices, and components of physical security controls within the co-location data centers. Physical security controls of the colocation data center are the responsibility of the data center service provider. The controls are monitored annually through onsite visits and the review of third-party audit reports.

CORPORATE OFFICES/SECURED FACILITY - Physical access to the facility and computer equipment located at corporate facilities is managed through the use of badge readers at all entry and exit points. The badge system is configured to log all card swipes. The badge system is configured to alert if doors are forced or if doors are held open for an extended period of time. Video surveillance is recorded and maintained for a minimum of 30 days to allow for a review.

TRAINING AND AWARENESS

1. How frequent are your employees who have access to school board data provided training with respect to privacy protection and security requirements of that data?

- Qualtrics employees are formally trained on company policies and security practices. This training occurs at the time of hire and at least annually through in-person or online for remote employees. In addition to the in-person trainings, regular updates are provided throughout the year through email, intranet postings, and regular company meetings. All employees are instructed to immediately report possible security incidents to their manager, InfoSec, and Legal.

2. How is this accomplished? What privacy legislation is referenced in that training (i.e. PIPEDA)?

- The computer security section of the employee manual includes the following topics:
    - Privacy law compliance
    - Physical security
    - Email acceptable use policy
    - Access control
    - Internet security
    - Personal devices in the company
    - Information Security Incidents
    - Password policy and tips
    - Insider threat