

Waterloo Region District School Board - Software Privacy and Security Standards

PRIVACY and SECURITY STANDARDS: MANDATORY – The following items are mandatory privacy and Security Standards required to provide Software to the Waterloo Region District School Board (the “Board”).

To become a Registered Software Vendor with the Board, it is mandatory that a signatory for your company responds in full compliance to the mandatory items noted below. If your company cannot comply with any of the standards, your registration will be denied.

1.0 Accountability and Responsibility

1.1 I/We acknowledge our responsibility to comply with Ontario/Canadian privacy legislation.

2.0 Data Collection

2.1 I/We will collect personal information only as defined in the agreement and authorized by the board.

2.2 I/We acknowledge that I/we are the trustees of the data; the data is owned by the board.

2.3 I/We must notify users when cookies are used as part of the provided service.

2.4 I/We must not use tracking cookies (i.e., cookies for 3rd parties and targeted advertising).

3.0 Data Use, Disclosure, and Retention

3.1 I/We may only use the data for the purpose(s) defined by the agreement/board, and for no other purpose.

3.2 I/We will disclose all third party data processors, subcontractors and services they employ along with the specific data elements involved and what protections/assurances are in place. This requirement is ongoing. I/We must notify the board of any changes or new third parties prior to making changes.

3.3 Where requested by the board, I/We agree to the transfer of data upon completion of the term of the contract or upon the dissolution of the contract to ensure there is no interruption of service.

3.4 I/We retain data for a period as determined by the board (indefinite retention is not acceptable) and agrees to securely dispose of data at the end of the prescribed retention period as verified by a certificate of destruction.

3.5 I/We ensure data collected is kept secure and separate from the data of other customers.

4.0 Security

- 4.1 I/We perform regular audits and threat risk assessments and will make available audit results upon request.
 - 4.2 The Board reserves the right to audit data security practices.
 - 4.3 I/We have a breach response protocol in place and will submit a copy upon request.
 - 4.4 I/We will notify the Board in the event there is a data breach and will require all third parties to notify the us and the Board in the event of a breach of board data.
 - 4.5 I/We will notify the affected parties in the event there is a data breach.
 - 4.6 I/We will cooperate with the Board in the event of a regulatory investigation (i.e., breach investigation by the IPC).
 - 4.7 I/We will notify the Board when I/We change our security measures/practices.
 - 4.8 I/We confirm that the Board is indemnified against 3rd party claims.
-