Waterloo Region District School Board

Administrative Procedure 4790

CLASSIFICATION AND SECURITY OF DATA

Responsibility:	*Director of Education*
Legal References:	*Municipal Freedom of Information and Protection of Privacy Act* *Personal Health Information Protection Act* *Personal Information Protection and Electronic Documents Act*
Related References:	*BP 1014 - Freedom of Information and Records Management* *AP 1100 - MFIPPA* *AP 1104 - Privacy Breach Protocol* *AP 4770 - Secure Disposition of Records* *WRDSB Record Retention Schedule* *AP 4070 - Responsible Use Procedure for Information, Communication and Collaboration Technologies* *AP 4081 - ITS Server Hardening* *Information Technology Remote Network Access: Internal ITS Procedure*
Revisions:	May 2020
Reviewed:	May 2020

1. Preamble

The Waterloo Region District School Board (WRDSB) strives to model and teach the safe, legal and responsible use of information, technology and resources. With this comes a duty to protect staff, student and confidential corporate information and to prevent the potential misuse of data by accidental or intentional means. The WRDSB follows the information privacy regulations set out in the *Municipal Freedom of Information and Protection of Privacy Act* and other privacy legislation.

2. General

2.1 Within the WRDSB, it is understood that some information is more sensitive than other information. The more sensitive the data, the more it needs to be protected in a secure manner.

2.2 It is further understood that there are some business processes which require data to be exchanged with parties outside of the Waterloo Region District School Board. These exchanges of data need to occur with a level of security appropriate to the sensitivity of the data.

3. Definitions

3.1 Data Owners: Those individuals who create and/or who have direct responsibility for the data.

3.2 Data Custodians: Those individuals whose responsibility it is to protect, and manage access to the data. These are often Information Technology Services staff.

3.3 Data Consumers: Individuals who use the data. Data consumers have an obligation to protect data and to use it appropriately.

4. Determining Information Sensitivity

4.1 Data owners and data consumers are responsible to determine the sensitivity level of data and utilize the appropriate security measures to ensure confidentiality and integrity, if required by the data.

4.2 The chart below should assist in determining the level of sensitivity of certain types of information. The examples are not meant to be all-inclusive, but rather to provide a sampling of data that would fall in that particular category.

Level of Sensitivity	Ways to Protect the Information	Examples of Information
Low Sensitivity	● No need to protect the information. The information is publicly-available.	● Corporate or school websites ● Minutes of Board and Committee of the Whole meetings ● General information around enrolment (e.g. numbers of students) ● Published financial statements and budget documents ● Most procedures, except those that provide safety or security information (i.e. bomb threat procedure).
Medium Sensitivity	● Share the information on a “need to know” basis ● Limit the number of copies of the information ● Password protect the data where possible ● Destroy the information in a secure manner when no longer required ● Review the privacy policies of the provider to see how the data is protected	● E-mail messages that do not contain any personal or confidential business information ● Student collaborative work on projects ● Agendas and minutes of meetings
High Sensitivity	● Password protection ● Data Encryption ● Non-disclosure ● Shred the data when no longer required ● Only use cloud solutions with robust privacy agreements such as Google Apps for Education or Microsoft 365—not publicly-available applications	● Student data (e.g. personal, medical, family, achievement, demographic information etc.) ● Staff data (e.g. personal, medical, absence, payroll or demographic information etc.) ● Confidential financial or other corporate data ● In-camera Board meeting minutes ● E-mail messages containing personal or

		confidential business information ● Procedures that contain safety or security information

Protecting Data Held Inside the WRDSB Network

5.1 The WRDSB internal network environment provides for administrative and instructional user accounts, personalized staff and student log-ins and access to a variety of core applications. Data is filtered through the Board's firewall, through specific security applied to each user account and through the Active Directory authentication process. Data is backed-up at regular intervals for business continuity purposes. As a further safeguard, only Board-approved administrative and instructional hardware is able to connect to the internal network.

5.2 Highly sensitive data residing on internal servers must have appropriate security and access controls wherever possible. When highly sensitive data resides or is transmitted to external servers or vendors, a non-disclosure agreement must be in place with the vendor and extra security measures must be taken, such as encryption and/or password protection during data access and transfer.

6. Protecting WRDSB Data Held Outside the WRDSB Network

Staff and student email/accounts

6.1 Hosted service locations which are outside of the WRDSB network (sometimes referred to as "cloud computing"), includes such services as personal email servers (e.g. Gmail), document management sites (e.g. Google Apps for Education (GAFE), Google Docs or survey tools).

6.2 The Ministry of Education has offered agreements with Google and Microsoft to provide a more secure "walled garden" cloud environment for school boards to use. The WRDSB has opted to use the Google Apps for Education "walled garden". Students and/or staff log into the Board's secure space (google.wrdsb.ca) using their Active Directory login (their PAL or PIL account).

Shared Documents/Drives

6.3 Privacy and access settings can be applied to individual documents and shared on a"need to know" basis. Additional information can be found in GAFE guideline documents. Within the Board's Google Apps for Education space, it is acceptable to include personally-identifiable information about staff or students or other confidential business information. It is not acceptable to include personally-identifiable information in other publicly-available cloud applications. G-Suite Privacy Considerations.

6.4 All laptop devices distributed by the Board are encrypted with Bitlocker encryption.

Third Party Vendors

6.5 Data which is shared with third party vendors who provide services for the Board (e.g. Student Information System, Human Resources Information System) may require uploads of information in order to perform the contracted services.

6.5.1 Data Sharing Agreements

When this is necessary, consideration must be given to the sensitivity of the required data prior to any exchange of information. Following current privacy legislation such as the *Municipal Freedom of Information and Protection of Privacy Act, Personal Health Information Protection Act* or the *Personal Information Protection and Electronic Documents Act*, the contractual agreement with the vendor must include appropriate language to protect personal or confidential information, and the appropriate consents must be obtained, if required.

6.5.2 Software Privacy and Security Standards Review

When the data is considered to be Highly Sensitive, there need to be safeguards in the contract and at the vendor's physical location to protect the information. Schools and other locations should work with staff in Procurement Services to ensure that the appropriate language is contained in contracts when vendors complete a Mandatory Software Privacy and Security Standards.

6.5.3 Secure Data Transfer Methods

Where a situation arises with the need to share data with a Vendor, this data will be archived into a password encrypted file for transfer over a SFTP protocol only. This is outlined in the IT Sharing Data with Vendors Process.

A non-disclosure agreement, in collaboration with Procurement, will also have been completed prior to sharing this data.

6.5.4 Use of Encryption

All data that is shared with approved vendors shall be encrypted using an archive zip tool and password protected as outlined in the Sharing Data with Vendors process.

6.5.5 Data in Transit

Recognizing that all data encompasses some level of privacy, all data in transit is encrypted via an encryption certificate that encrypts the data on the application server.

All systems that deliver data must use an encryption method such as a certificate, that is available from the Security Analyst when requested via a Request Ticket.

Test Data Management

6.6 The TEST and BETA Databases replicates the data from the Production environment through a controlled and repeatable process using stored procedures.
In all other instances where a test database requires a refresh of data, an export is generated from the production database, and imported into the respective TEST database. This process also ensures that the backup strategies in place are validated.

The users are limited to specific developers and authorized staff for testing upgrades. This process is outlined in the Test Database Management process.

7. Use of Mobile or Portable Devices

7.1 The use of any type of mobile or portable device (e.g. Smart Phones, tablets, memory sticks, flash drives, laptops) which hold or transport data must consider the type(s) of data which may be contained on the device.

If the device contains data with High Sensitivity, then the device must have the proper protections in order to secure the data, such as strong device password protection and device encryption. Smart phone users must password-protect their devices, according to the information received in their training.

8. Privacy Breaches

8.1 A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are inconsistent with existing privacy legislation. Often, breaches occur as a result of human error and personal information is released to individuals or organizations who should not be in receipt of the data. Data considered to have “High” sensitivity needs to be safeguarded at all times. If a privacy breach is suspected, AP1104 Privacy Breach Protocol, provides direction to staff on containment, assessment and notification of privacy breaches.

9. Retention of Data

9.1 Corporate data in all forms (hard copy, electronic, microfilm) is retained according to the Board’s current Records Retention Schedule and then destroyed in a manner appropriate to the type of information. AP4770 Secure Disposition of Records, can provide additional information on the secure disposition of records.

9.2 Questions about the sensitivity of specific types of information or retention can be directed to the Freedom of Information, Privacy and Records Information Management Officer.