

Western Québec School Board Administrative Directive

Use of Unsanctioned Communication Tools for Parent Communication

Effective Date: August 26, 2026

Ref: #2026/27-01

Summary

Teachers and other employees must use WQSB-approved communication tools, including Board email, Microsoft Teams, and the Mozaïk Teacher Portal (Clic-école), for electronic parent communications. Personal communication platforms, unsanctioned applications and platforms as well as social media messaging applications are not authorized for school-related communications between teachers and parents/guardians nor between teachers and students.

1. Purpose

The directive aims to establish standards governing the use of communication platforms for teacher-parent communications that comply with recent privacy legislation, cybersecurity requirements, records retention obligations, and WQSB policies. More specifically, this directive is established to prevent the distribution of personal information.

2. Scope

This directive applies to all WQSB employees who communicate with parents, guardians, or students in the course of their professional duties, including but not limited to teachers, administrators, professionals, and support staff. It applies to the direct transmission of messages to individual parents / guardians or to a group of parents / guardians. It does not concern the promotional or institutional information that is posted on schools' and centres' official websites and social media platforms.

3. Authorized Communication Platforms

The following WQSB-approved communication platforms shall be used for direct communications between school personnel / centre personnel and parents/guardians:

- WQSB-issued email accounts;
- Microsoft Teams and associated Microsoft 365 services authorized by the School Board;
- Mozaïk Portal and associated communication modules approved by the School Board; and;
- Any other platform that has been formally approved by the WQSB after a privacy impact assessment has been conducted according to privacy legislation.

4. Prohibited Use of Non-Authorized Platforms

Employees shall not use personal, third-party, or non-authorized communication platforms to conduct school-related communications with parents or guardians unless expressly authorized in writing by the School Board.

This prohibition includes, but is not limited to:

- Personal email accounts, personal text messaging services, Facebook Messenger, WhatsApp, Signal, Telegram, Instagram Direct Messages, Snapchat, Discord, WeChat, Edmodo, Seesaw, Remind, Class Dojo, Personal websites, Personal social media accounts, and any platform not approved through the Board's information security and privacy review process.

5. Rationale

The Western Québec School Board (WQSB) is committed to maintaining effective, secure, professional, and accessible communication between school personnel and parents/guardians.

The School Board must ensure that communications involving students, parents, and educational matters are conducted through platforms that provide appropriate safeguards and administrative oversight.

The use of non-authorized platforms presents significant risks, including:

- Unauthorized disclosure of personal information;
- Non-compliance with privacy legislation and access-to-information requirements;
- Cybersecurity vulnerabilities.

This directive also aims to reduce the number of communication tools and applications needed by parents/guardians to receive communication from various employees at their child's/children's school. This aligns with the commitment outlined by the Ministère de l'Éducation during its Clic-école campaign in 2025-2026.

6. Responsibilities

Employees are responsible for:

- Using only approved communication platforms;
- Protecting the confidentiality of student and parent information;
- Reporting any unauthorized disclosure or security concern to their supervisor and the Information Technology Department; and
- Complying with all School Board policies and directives related to privacy, cybersecurity, and records management.

Principals, Centre Directors and Supervisors are responsible for:

- Communicating this directive to staff;
- Monitoring compliance within their school, centre or department;
- Addressing concerns related to unauthorized communication practices; and
- Seeking guidance from Corporate Services, Communications, Human Resources, or Information Technology where required.

The Information Technology Department is responsible for:

- Maintaining secure communication systems;
- Providing guidance regarding cybersecurity and privacy requirements;
- Conducting Privacy Impact Assessments for new tools under review.

The Secretary General (Responsible for the Protection of Personal Information) is responsible for:

- Receiving requests for approval of communication tools;
- Referring the requests to the Committee for the Protection of Personal Information

The Committee for the Protection of Personal Information is responsible for:

- Reviewing the requests to approve the sanctioning of communication tools;
- Requesting the Information Technology Department to conduct Privacy Impact Assessments for communication tools;
- Approving the request to sanction communication tools.

7. Non-Compliance

Failure to comply with this directive may result in disciplinary action in accordance with applicable School Board policies, collective agreements, employment conditions, and relevant legislation.

8. Review

This directive shall be reviewed periodically and updated as required to reflect changes in legislation, technology, cybersecurity standards, and operational requirements.