RISK APPETITE STATEMENT

This Risk Appetite Statement outlines the level of risk the Board is willing to accept in pursuit of its mission, values and priorities. It guides decision making, resource allocation, and mitigation planning.

The Board's overall risk appetite is conservative because, as a school division, its decisions directly affect students, staff, schools, and the broader community, requiring risks to be carefully considered and responsibly managed. The Board will not knowingly accept risks assessed above a Moderate level unless exceptional circumstances exist and explicit Board approval has been obtained, supported by documented mitigation strategies and ongoing monitoring.

Risk appetite is reviewed annually and may be adjusted based on emerging risks, legislative changes, or strategic priorities.

Risk Appetite Definitions

Appetite	Definition
Very Low	The Board has little to no tolerance for risk and expects risks to be avoided wherever possible.
Low	The Board accepts limited risk where there is a clear rationale and appropriate safeguards are in place.
Moderate	The Board recognizes that achieving Division objectives may require accepting a measured level of risk.

Risk Appetite Levels

Category	Appetite	Description	Examples
Student Safety & Well-Being	**Very Low**	The Division will not accept risks that compromise physical, emotional, or psychological safety.	Unacceptable: delayed response to safety threats. Acceptable: operational inconvenience to enhance safety.
Student Learning & Outcomes	**Low**	The Division accepts limited risk that could negatively impact student learning outcomes and achievement.	Unacceptable: sustained gaps in instructional quality without intervention.

Category	Appetite	Description	Examples
			Acceptable: piloting new instructional approaches with monitoring and evaluation.
Privacy & Access to Information (POPA/ATIA)	**Very Low**	The Division will not accept risks that could lead to unauthorized disclosure of personal or confidential information.	Unacceptable: weak access controls. Acceptable: multi-factor authentication (MFA) delays.
Governance & Compliance	**Low**	The Division avoids risks that could result in non-compliance.	Unacceptable: non-compliance with ATIA timelines. Acceptable: implementing interim procedures while adapting to new legislative or regulatory requirements.
Information Technology & Cybersecurity	**Low**	The Division limits risks that could disrupt operations, compromise systems, or expose digital assets to cyber threats.	Unacceptable: inadequate system security controls. Acceptable: short-term service interruptions during system upgrades.
Reputation	**Low**	The Division avoids risks that could significantly damage public trust.	Unacceptable: unmanaged communication during incidents. Acceptable: taking time to confirm facts before communicating with partners to ensure information is accurate and transparent.
Facilities	**Low**	The Division has low tolerance for risks that compromise the safety, functionality, or regulatory compliance of facilities.	Unacceptable: deferred maintenance creating safety hazards. Acceptable: short-term service disruptions during planned upgrades.
Finance	**Low–Moderate**	Some risk may be accepted to pursue innovation or operational improvements.	Unacceptable: material budget overruns or financial commitments without appropriate oversight. Acceptable: pilot projects with limited exposure.

Category	Appetite	Description	Examples
Human Resources	**Moderate**	Moderate risk may be accepted due to labour market constraints.	Unacceptable: compromising employee qualification screening requirements to address staffing shortages. Acceptable: temporary staffing shortages with mitigation.
Operations & Continuity	**Moderate**	The Division accepts some operational risk where continuity plans and mitigation strategies are in place.	Unacceptable: lack of preparedness for foreseeable disruptions. Acceptable: service disruptions with contingency planning.