PRIVACY TALK SPECIAL TOPIC – PRIVACY AND GENERAL RISKS PERTAINING TO AI

When using Generative AI tools, safety, security, and privacy must be at the forefront for all employees. Please consider the following when using AI tools to assist you in your role:

Safety, Security, and Privacy Considerations:

- Personal information is defined as **recorded information about an identifiable individual** (i.e., OEN, education or medical information, family status);
- Do not put personal information about individuals into any AI tool;
- Do not use any AI tool when dealing with fellow employees and employment-related matters that include personal information;
- Avoid using any AI tool for work if not using a board-issued device.

Privacy and generic risks to consider regarding AI:

- AI Models may leak, generate, or correctly infer sensitive information about individuals, which can present significant privacy risks*;
- AI models may also be able to infer personal information or sensitive data that was not in their training data nor disclosed by the user by combining information from different sources*;
- Lowered barriers to entry can generate and support the exchange and consumption of content which may not distinguish fact from opinion, questioning information integrity;
- Lowered barriers for offensive cyber capabilities may exist, including exploiting vulnerabilities to ease hacking, malware, phishing, offensive cyber operations, or other cyberattacks, possibly compromising information security.

Legislation: Be aware of all relevant regulations such as Ontario's Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), which guides how privacy protections are implemented and managed as well as the Education Act, and the Ontario College of Teachers Professional Standards.

***Risks noted in NIST AI 600-1: Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile**

Guidance:

- Users of AI should be prepared to disclose and report on its use when asked. This includes understanding how and when AI is being used and ensuring that AI use is transparent and accountable;
- Use AI tools in a manner consistent with Board Policies and Administrative Operational Procedures;
- Report concerns or incidents involving AI to the Principal;
- AI is a tool, not a perfect solution. Think critically about its outputs and question the information created. Stay curious and use AI to complement work, not over-rely on it, understand its limitations.

Please adhere to **P&I Memo 1491 Approved Board-Wide AI Guide Now Available** which lists approved AI tools for staff. Niagara Catholic cannot guarantee the security of the information when third-party AI applications are used.