

Vetting of Application Security & Privacy

About ECNO

The Education Collaborative Network of Ontario (ECNO) is proud and fortunate to play an important role in the education system by providing information technology leadership for Ontario's K-12 educators to empower student success while enabling school Board efficiencies and savings.

As we embrace more change in how we teach, learn, and communicate, there will be critical need for innovative IT leadership that empowers student success while ensuring privacy and safety.

ECNO has a variety of products and services to help Ontario school Boards meet these needs.



www.ecno.org
office@ecno.org | (519) 568-7899

ECNO is a virtual organization.



Summary of Service

In response to requests from Ontario K-12 school Boards, ECNO, in collaboration with the OASBO Joint Committee, established the **Vetting of Application Security & Privacy (VASP)** shared service. VASP centrally provides professional risk assessments of security and privacy concerns related to educational digital tools and applications on behalf of participating Ontario K-12 school Boards.

Our process for assessing applications is based on our Student Digital Privacy Standard. This ensures that web apps, software, and online services used in Ontario school Boards adhere to uncompromising high standards of protection and embodies progressive privacy and security protections that align with those endorsed by regulators and experts across North America and the European Union. This standard is intended to shift the data protection landscape and raise the bar for student digital privacy in Ontario schools, ensuring a safe learning environment for all.

What it is

Prior to submitting a request for VASP to conduct an assessment, Boards conduct their own internal assessment of their digital tools and applications from a pedagogical lens, and establish that the Board has the infrastructure to support the software. The Board then submits a request for VASP to assess it.

The application is initially assessed by one of the privacy/security teams. The Privacy Analyst vets the supporting documents and the Security Analyst ‘fuzzes’ the application. Typically, the vetting and fuzzing process results in a set of questions and recommendations for the provider. VASP shares these with the provider.

Following provider discussions, the analysts produce school Board and Educator reports based on the initial assessment along with any changes/clarifications obtained during discussions with the provider.

How it works

Each assessment examines the student information being collected, weighing any privacy or security risks, verifying compliance between publicly stated policies/terms and practice, and advising on mitigating strategies where required. Following completion of each review, two assessments are produced in both English and French:

- School Board report:** a technical report to provide centralized IT, curriculum, and procurement staff with a risk score and information about the risks the Board should consider, and any mitigating strategies that can help reduce the identified risks.
- Educator report:** plain language information for educators and school administrators about how to implement/use the digital tool or application, while minimizing risks where possible.

How it helps

VASP's value comes from our ability as a third party to provide standard-based security and privacy assessments for Ontario school Boards. In doing so, we create efficiencies for both the school Boards and the Providers. Prior to VASP, each Board had to conduct their own individual assessments and reach out to providers on their own, leaving providers to respond to them all separately. VASP produces a single assessment based on their professional experience that is available for all Boards to use.

The VASP assessments provide Boards with a risk score, incorporating information about the risks that should be considered, and any mitigating strategies that can help reduce the identified risks. VASP does not approve or disapprove of the use of a digital tool or application. It is ultimately up to each Board to assess the risks identified against their tolerance in deciding whether or not to use an application.

