

Provincial Privacy of Student Information Policy

Effective Date: July 2016

To ensure you are accessing up-to date information, please refer to the online version of this policy at ednet.ns.ca/document-depot.

1. Policy Statement

School boards collect, use, and disclose student personal information to support the provision of educational services to their students. School boards must uphold the principles of privacy, good custodianship, and accountability when collecting, using, and disclosing this information.

School boards must also respect the privacy and intellectual property of students in the publication of personal information and student work, and will only publish student personal information and student work in accordance with this policy.

2. Definitions

“Consent” means the written, informed consent by a student 19 years or older, or by the parent or legal guardian of a student under the age of 19 (see Appendix A: Consent for Publication of Student Personal Information and Student Work).

“Copyright” means the exclusive legal right, given to the creator of a literary, artistic, or musical work, to print, publish, perform, film, or record it, and to authorize others to do the same. Students are the creators of their student work.

“Copyright Act” means the federal statute governing copyright law in Canada ([Copyright Act](#))

“Department” means the Nova Scotia Department of Education and Early Childhood Development.

“Digital resource” means an electronic document or file such as a video or audio file, or a text-based file such as a Word document or PowerPoint presentation.

“Employee” means an individual in the employ of, seconded to, or under personal service contract with the school board.

“FOIPOP” means the [Freedom of Information and Protection of Privacy Act](#). This act ensures that public bodies are open and accountable to the public by providing a right of access to records, and protects the privacy of individuals by controlling the manner in which public bodies collect, use, and disclose personal information.

“Personal information” is defined in clause 3(1)(l) of the FOIPOP Act, “recorded information about an identifiable individual”, including:

- (a) the individual’s name, address or telephone number,
- (b) the individual’s race, national or ethnic origin, colour, or religious or political beliefs or associations,

- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health-care history, including a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinion about the individual, and
- (i) the individual's personal views or opinions, except if they are about someone else

For greater clarity, personal information includes images of an identifiable individual.

"Privacy breach" means the event of unauthorized collection, access, use, disclosure, or alteration of personal information.

"Privacy Impact Assessment" means a process that identifies, addresses, and documents potential privacy risks that may occur in the course of collecting, using, or disclosing personal information.

"Publish" means to release or make students' personal information and/or student work accessible to the public.

"Student work" means intellectual property created by the student individually or as a contributor to a group project.

"Volunteer" means an individual who gives their time or effort to a school and does not receive payment for that work.

3. Policy Objectives

This policy is designed to ensure that school boards understand their responsibility to comply with provincial and federal legislation related to the protection of privacy, the disclosure and/or publication of student personal information, and the use and publishing of student work. This includes

- the protection of personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal;
- obtaining the written, informed consent of an individual when personal information or student's work is published in any format, to respect privacy, copyright, and the intellectual property of others; and
- those authorized to access such information are only doing so for specific and legitimate work purposes, for example, as outlined in the [Student Records Policy](#).

4. Application

The [Freedom of Information and Protection of Privacy Act](#), the [Personal Information International Disclosure Protection Act](#), and the [Copyright Act](#), require all school boards to comply with the protection of personal information provisions and the intellectual property provisions of these acts. The directives and guidelines for student information outlined in this policy align with these acts.

This policy applies to all school boards, their employees, and volunteers.

5. Policy Directives

School boards will distribute the Provincial Privacy of Student Information Policy to all their employees and volunteers.

School boards must only collect, access, use, disclose, and dispose of student personal information where authorized by law.

5.1 Privacy Breach Protocol

School boards shall have a privacy breach protocol that contains at minimum the requirements as outlined in Appendix B. The privacy breach protocol will determine the steps that will be followed when a school board learns of a possible breach of student personal information.

5.2 Access and Security

Student personal information must be maintained securely and be accessible only to the employees or volunteers who need access to the information for the purpose of carrying out a program or service of the school board. For example, student personal information in paper format will be stored securely and protected against unauthorized access; student personal information in electronic format will be password-protected and have adequate controls in place to ensure the confidentiality, integrity, and availability of information to specified users only. This includes all electronic data including email, USB keys, cloud storage, and servers.

Disposal of transitory and master records containing student personal information will be carried out using secure methods such as shredding. Student records shall be maintained in accordance with the [Student Records Policy](#).

5.3 Use of Consent Form

The Consent for Publication of Student Personal Information and Student Work form (see Appendix A) documents parent/guardian consent for the publishing of student personal information and student work. School boards shall ensure that the publication or posting of students' personal information and/or student work in school board materials, on the school board website, or in publications, is done only with written consent.

5.4 Training

Information and awareness will be provided to all employees and volunteers on the protection of student personal information, the need to respect the privacy rights, copyright, and intellectual property of others.

5.5 Privacy Impact Assessment

School boards may complete a Privacy Impact Assessment for any new program or service, or for any significant change to an existing program or service, that involves the new collection, use, or disclosure of student personal information as defined by the FOIPOP Act.

6. Roles and Responsibilities

The Department of Education and Early Childhood Development is responsible for

- communicating this policy to each school board

The School Boards are responsible for

- distributing the Provincial Student Information Privacy Policy
- advising all employees and volunteers who have access to student personal information on the collection, access to, use, and publication of that information and student work
- ensuring the publication of students' personal information and student work on the public school system's network and in school materials or publications is done with written consent
- monitoring compliance with this policy within their school board and ensuring appropriate responses are taken if there is a lack of compliance
- ensuring the use of digital resources within schools is consistent with the provisions of this policy and the [Personal Information International Disclosure Protection Act](#)

Principals are responsible for

- obtaining consent for the publication of student personal information and student work (see Appendix A: Consent for Publication of Student Personal Information and Student Work)
- ensuring that publication of students' personal information and student work on the public school system's network and in school materials or publications is done in accordance with the consent forms
- monitoring compliance with this policy within their school and taking appropriate response if there is a lack of compliance
- ensuring the use of digital resources within the principal's school is consistent with the provisions of this policy and the [Personal Information International Disclosure Protection Act](#)

Employees are responsible for

- ensuring that consent has been obtained before publishing students' personal information or student work
- ensuring the use of digital resources within the classroom is consistent with the provisions of this policy and the [Personal Information International Disclosure Protection Act](#)
- informing students about and modelling compliance with Canadian copyright law and respecting their own and others' intellectual property rights
- accessing and using student personal information is done in compliance with this policy, other relevant policies, and legislation

7. References

This policy operates along with and as a supplement to existing statutes, policies, guidelines, and regulations governing the collection, use, and disclosure of personal information, including the following:

Canada. Copyright Act. R.S.C. 1985, c. C-42. <http://laws-lois.justice.gc.ca/eng/acts/C-42/>.

Nova Scotia. Education Act. S.N.S. 1995-1996, ch. 1. <http://nslegislature.ca/legc/statutes/education.pdf>.

—. Freedom of Information and Protection of Privacy Act. S.N.S. 1993, ch. 5. <http://nslegislature.ca/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf>.

—. Ministerial Education Act Regulations. S.N.S. 1995-1996, ch. 1. <https://www.novascotia.ca/just/regulations/regs/edmin.htm>.

—. Ministerial Freedom of Information and Protection of Privacy Act Regulations. S.N.S. 1993, ch. 5. <https://www.novascotia.ca/just/regulations/regs/foiregs.htm>.

—. Personal Information International Disclosure Protection Act. S.N.S. 2006, ch. 3. <http://nslegislature.ca/legc/>.

—. Privacy Review Officer Act. S.N.S. 2008, ch. 42. <http://nslegislature.ca/legc/statutes/privacro.htm>.

—. 2009. Wide Area Network Security Standards. Halifax, NS: Province of Nova Scotia. https://icts.iweb.gov.ns.ca/wan_security/policy_documents/155.

Nova Scotia Department of Education and Early Childhood Development. n.d. Privacy Breach Protocol. Halifax, NS: Province of Nova Scotia. <https://www.ednet.ns.ca/files/foipop/Privacy%20Breach%20Protocol.pdf>.

—. 2016. Public School Network Access and Use Policy. Halifax, NS: Province of Nova Scotia. <https://www.ednet.ns.ca/sites/default/files/pubdocs-pdf/public-school-network-access-and-use-policy.pdf>.

—. 2006. Student Records Policy. Halifax, NS: Province of Nova Scotia. <http://studentservices.ednet.ns.ca/sites/default/files/StudentRecordsPolicy.pdf>.

8. Monitoring

The department will monitor this policy, including evaluating its suitability and effectiveness, and ensure that the policy is reviewed every two years.

9. Appendices

Appendix A: Consent for Publication of Student Personal Information and Student Work

Appendix B: Minimum Requirements for a Privacy Breach Protocol

Appendix A

Consent for Publication of Student Personal Information and Student Work

From time to time, the schools, school boards, and the Department of Education and Early Childhood Development would like to publish examples of student work, or personal information about a student such as the student's name, photograph, and school attended. This is done to recognize and encourage student achievement or learning, and to inform others about the school and its programs and activities. Showcasing students, their work, and their achievements is an important part of school life, and is a very positive experience for students.

- Before the school, school board, or the department does these things, we need your permission. Please sign this form to let us know whether or not you give your permission.

School and School Board Examples

Here are some specific examples of how the school or school board would like to publish student personal information or student work, in printed materials, electronic documents, and websites:

- Student artwork may be used on a school or school board website.
- Names and images of students may be published in a school yearbook.
- A student's academic or athletic achievements may be published in a school newsletter or on the school website, including social media like Twitter and Facebook.
- A student's photo and identifying information may be shared with newspaper or television media, or students may be photographed or interviewed by the newspaper or television media.
- A student may be videotaped by other students as a class project, or classroom activities may be videotaped and shown to teachers for their professional development.
- Pieces of student writing may be shown to teachers for professional development purposes, without the student's name or other identifying information.
- An individual student or a group of students may be photographed and the photograph may appear on the website of the school or school board.

Department Examples

Here are some specific examples of how the Department of Education and Early Childhood Development would like to publish student personal information or student work, in printed materials, electronic documents, and on its website:

- Pieces of student writing may be shown to teachers for professional development purposes, without identifying the student.
- A photo of an individual student or a group of students may be presented in a publication or on its website.



I consent to the school, to the [name of school board], and the Nova Scotia Department of Education and Early Childhood Development publishing my child's name, image (photo), grade, course, and school attended, including being photographed or interviewed by the media.

I also consent to the [name of school board] publishing my child's student work, and the department using my child's student work (such as student writing) for the purposes of teacher professional development, and photos in a publication or on its website.

This consent is limited to the purposes of recognizing and encouraging student achievement, teacher professional development, building school community, and informing others about the school and its programs and activities.

I understand that I may withdraw this consent at any time by contacting my child's school principal, in writing. This consent is valid for one year after the date of signing.

Yes, I consent

No, I do not consent

Name of student: _____

School attended: _____

Signature of parent/guardian
(or student if 19 years of age or older): _____

Date: _____

If you have any questions or concerns about how the school, school board, or the department is managing information about your child, or about anything in this consent form, please contact your child's principal, or the school board's information access and privacy officer.

Appendix B

Minimum Requirements for a Privacy Breach Protocol

Purpose

The purpose of this protocol is to outline the steps that must be followed when [school name / school board] learns of a possible breach of personal privacy. It will assist the [school name / school board] in controlling the situation and ensuring that, if a breach of privacy occurs, steps will be taken to prevent a similar breach from happening again.

Scope

This protocol applies to employees of [school name / school board], volunteers, students, and interns.

Background

A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with the provisions of the Freedom of Information and Protection of Privacy Act. The most common breach of personal privacy is the loss or unauthorized disclosure of personal information, for example through theft of a computer or handheld electronic device, or because an email was sent to a wrong address.

How to Respond to a Breach or Suspicion of Breach

1. Identify the privacy breach

Identify and record the date, time, location, length, type, and extent of the breach.

2. Take immediate remedial action

Identify what action is necessary to contain or stop the breach. For example:

- Retrieve hard copies of personal information, or if that is not practical, the recipient(s) must confirm that the hard copies were securely disposed.
- Recall unopened Outlook email. For email that has been opened, request the email be deleted and hard copies be securely destroyed.
- For recipient(s) not on Outlook, contact the recipient(s) to request deletion of the email and secure disposal of any hard copies.
- Request that electronic copies of any personal information that has been disclosed be deleted from the individual's desktop computer, server, and any other storage device or media.
- Determine whether the breach will allow access to any other personal information, and if so, take steps to avoid this potential additional breach.
- Determine whether the breach will allow unauthorized access to any other personal information (e.g., an electronic information system). Take whatever necessary steps are appropriate (e.g., change passwords, identification numbers, and/or temporarily shut down a system).
- If an electronic device and paper records containing personal information was stolen, contact security (if within the [school name / school board]) and/or the police (if outside the [school name / school board]).

3. Investigation and documentation

Determine the detail of what and whose personal information is involved, and what the extent/scope of the breach is. Sample questions:

- Were the immediate remedial actions effective?
- Is there enough documented evidence about the incident to determine the series of events that led to the breach?

4. Internal notification

Identify who must be notified when a breach is suspected, and the notification process that must be followed (e.g., who should be notified first, and who is responsible for notifying each individual).

5. External notification

Identify who must be notified when a breach is suspected, and the notification process that must be followed (e.g., who should be notified first, and who is responsible for notifying each individual).

6. Follow-up and long-term remedial action

Determine what follow-up and long-term remedial action there will be to prevent the breach from occurring again, e.g., report with analysis and listing of future preventive measures. Example questions include:

- Was the privacy breach protocol followed?
- Are new or amended policies, procedures, and/or training required to prevent reoccurrence of the breach?
- What plans have to be developed to lessen the likelihood or eliminate the possibility of another breach?