Office of the Information and Privacy Commissioner for Nova Scotia

Guidance for the Use of Criminal Record Checks By Universities and Colleges

This guidance document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. It is intended to assist universities and colleges in deciding whether or not the organization has the authority under Nova Scotia's privacy legislation to collect, use, and disclose criminal record checks from students and potential students. It also makes 17 best practice recommendations for how to implement a criminal record check program.

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with the *Freedom of Information and Protection of Privacy Act*, the Office of the Information and Privacy Commissioner (OIPC) cannot approve in advance any proposal from a public body. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner will keep an open mind. It remains the responsibility of each public body to ensure that it complies with its responsibilities under the legislation. Visit us at: www.foipop.ns.ca

Background

It came to the attention of the Information and Privacy Commissioner[1] that many colleges and universities ("schools") in Nova Scotia have made it a practice to collect criminal record checks from students, and potential students, for some of their program areas. This information is then used by the schools to make decisions about student placements for program practicums and in some cases whether or not the student will be admitted to the program at all.

One of the purposes of the *Freedom of Information and Protection of Privacy Act ("FOIPOP")* is to ensure that public bodies are fully accountable to the public by preventing the unauthorized collection, use or disclosure of personal information. Criminal record checks, by their nature, contain very sensitive personal information.

The following provides the rules and 17 best practice suggestions that schools should consider when deciding whether to collect, use or disclose criminal record checks as part of their admittance and placement processes.

COLLECTION

Collection Rules

Schools have identified that the authority they rely on, for the collection of personal information through criminal record checks, is that the information relates directly to and is necessary for an operating program or activity of the school.[2] Schools with programs that require a student practicum placement state that some employers (placement partners) require that any student placed with them for work experience must have completed a criminal record check. Where the practicum placement is a requirement for graduation, schools take the position that the criminal record check is therefore necessary for the school program – they must ensure students will be eligible for placement so they can complete the program.

Collection occurs when a school gathers, acquires, receives or obtains personal information. There is no restriction on how the information is collected, which can mean obtaining a physical copy or simply viewing it.

Schools must establish on a program-by-program basis whether or not they have the authority under *FOIPOP* to collect personal information regarding the criminal history of individuals. *FOIPOP* states that personal information may be collected if it "relates directly to and is necessary for an operating program or activity". Therefore, in order to have authority to collect the personal information, the school must establish three things:

1. To "relate directly to", the information must have a <u>direct</u> bearing on the operating program or activity of the college or university.
2. To be "necessary for" means that without the information the program (part of the school's mandate) or activity (steps to carry out the mandate) would not be viable.

---

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*. It is the role of the Commissioner to monitor how the privacy provisions are administered, by conducting investigations into compliance, undertaking research and informing the public.

[2] This is a purpose authorized by s. 24(1)(c) of *FOIPOP*. *FOIPOP* authorizes two other purposes – if an Act expressly authorizes it (s. 24(1)(c)) or if it is for law enforcement purposes (s. 24(1)(b)).

3. The collection must relate to an operating program or activity of the college or university, not to another organization (i.e. a placement partner).

A school that determines it does not have authority to collect must stop collecting the information. All criminal record checks that were collected previously should be destroyed in accordance with the school's records retention schedule and in accordance with *FOIPOP*.[3]

If a school establishes that it does have authority to collect personal information through criminal record checks, best practice is to then consider if it should proceed with collection and if so, to what extent. The following 17 best practices will help to guide colleges and universities in establishing a *FOIPOP* compliant program.

Collection Best Practices

Minimize. Schools should be careful to only collect the minimum amount of personal information that is necessary for the intended program or activity. This can be accomplished in two ways:

1. Conduct the least invasive form of check required: If only a criminal record check is required, ensure other forms of checks are not also conducted – such as a vulnerable sector check or a child abuse registry check.

2. Don't make copies: Schools only need to check if the criminal record check is "clean" or not. If the criminal record check is clean, it does not need to be kept at all. Schools should have a way to note on collection day that the criminal record check was viewed and was clean - a copy should not be retained.

   In cases where the record is not clean, an appointment should be set up with an advisor to discuss the student's options (see more below in "Use Best Practices").

Formalize. It is important to document the reasons for the collection of personal information. Best practices include:

3. Document placement partner requirements: If the primary reason for the criminal record check is because placement partners will only accept students who meet the organization's human resources requirements (a clean record or acceptable convictions only), formalize the expectation of each of the placement partners in writing. Documentation must include a list of relevant offences for each placement type to aid the school in deciding whether or not a student is eligible for placement.

4. Update expectations: The school should periodically confirm with each placement partner that their expectations remain the same and update the documentation as needed.

5. Develop employee guidance: Schools should develop appropriate written policies and procedures to guide their employees who are responsible for collecting and assessing the relevance of criminal record checks, and to ensure compliance with the privacy provisions of *FOIPOP*.

[3] Section 24(4) of *FOIPOP* states that when a public body uses personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year.

Notify. Whether or not a copy of the criminal record check is retained, a collection is occurring. Schools should have a notice of purpose available to students.

6. Notify and obtain consent from students: Provide a clear notification to students and applicants of the reason for the collection of criminal record check information. The notice should explain the purpose, nature and extent of collection of their personal information and should seek student consent for any intended uses or disclosures of the information.

USE

Use Rules

Schools have identified that the authority they rely on for using criminal record checks is that it is for the same purpose it was collected for - to assess the student's ability to be accepted into a practicum placement and program admittance.[4] However, as noted above, best practice is to obtain consent from students for the use of their personal information.

Accessing (looking at) personal information is a use. Schools should be careful to only use personal information for authorized purposes and should limit access to only those that require the information to do their jobs.

Use Best Practices

Formalize. It is important to document the reasons for the use of personal information. Best practice includes:

7. Develop tools: Create a conviction relevance matrix. For each program area list the relevant convictions based on the information supplied by employers.

Centralize. Centralize the decision making about a student's ability to be placed with a placement partner or accepted into a program based on his or her criminal history. This practice will achieve the following privacy supportive practices:

8. Develop expertise: Centralizing decision making will allow the person making decisions to develop expertise (including the development of a conviction relevance matrix).

9. Limit access: Only those who are making the decisions will have access to the sensitive information. In cases where the criminal record check is not clean, the student/potential student would book an appointment with the central criminal record check contact for further investigation. If that person cannot make a decision based on his or her understanding of the conviction relevance matrix, then a call can be made to the placement partner to discuss what it thinks in the form of a hypothetical question. If the placement partner is willing to accept the student, the process would move on. If not, the school would follow its screening process.

[4] This is a purpose authorized by s. 26(a) of *FOIPOP*. *FOIPOP* authorizes two other purposes – with consent (s. 26(b)) or if *FOIPOP* authorized another public body to disclose the information to the school (s. 26(c)).

DISCLOSURE

Disclosure Rules

FOIPOP provides for the disclosure of personal information with consent of the affected individual or in limited circumstances without consent. Disclosure includes the sharing of personal information with a placement partner. The school practices may vary in what is disclosed to placement partners about the criminal record checks.

Disclosure Best Practices

Don't disclose. Disclosure, even if authorized, is discretionary. Schools should consider the following when deciding if disclosure is appropriate:

10. Passage of time: Given placement generally happens well into the student's training, a criminal record check that was provided to the school prior to or just after beginning the program will be out of date (normally they are valid for six months). A lot can happen in a student's life during that time, so the criminal record check may no longer be accurate and therefore would not serve the purpose it is intended for.

11. Shift responsibility: The placement partner could make its own request to the student directly, identifying its own authority for collection and keeping in mind that it is no longer for the school's purposes, it is the placement partner's purposes. In this case, there would be no need for the school to collect any criminal record information.

Get consent. If disclosing the actual criminal record check to placement partners, ensure that consent is received from the student at the time of the disclosure. Keep in mind:

12. Informed consent: Having a student sign a blanket consent form at the beginning of the program will not generally be adequate. The consent to disclosure should be signed at or near the time of disclosure and should identify both the information to be disclosed and the organization to which the school is authorized to disclose the information.

Minimize. Schools should be careful to only disclose the minimum amount of personal information that is necessary for the intended purpose. This can be accomplished by:

13. Don't provide copies: Schools can simply confirm that the record is clean. Presumably any student who has not passed the internal school criminal record review process will not be offered as a placement student so there will generally be no need to disclose any negative criminal record information outside of the school.

SECURITY

Security Rules

FOIPOP requires[5] schools to have adequate security arrangements (administrative, physical, technical and personnel) in place to protect privacy.

Security Best Practices

Mitigate risk. Schools should understand what the privacy implications are when collecting, using and disclosing, storing and disposing of personal information. This can be achieved by developing a privacy management framework[6] that includes the following best practices:

14. Conduct an assessment: Prepare a privacy impact assessment ("PIA") to assess and mitigate privacy implications before beginning to collect, use or disclose criminal record check information.[7]

15. Limit access: Criminal record checks should be placed in locked cabinets, accessible to only people that are required to use the criminal record check as a function of their jobs.

16. Develop policy: Without written policies and procedures in place, schools have not taken responsible steps to safeguard personal information in their custody and control. Written policies and procedures will guide employees, who are responsible for programs that involve placements, to ensure compliance with the privacy provisions under *FOIPOP.*[8]

17. Records Management: Do not keep criminal record checks longer than necessary. Schools should develop a retention schedule and ensure it is followed. Keeping records longer than needed increases the risks associated with storing personal information (such as breaches).

[5] S. 24(3) of *FOIPOP*. See the OIPC website for the Security Checklist which provides some preliminary guidance on what practices meet the minimum security requirements under *FOIPOP* Reasonable Security Checklist for Personal Information.
[6] For more details on how to implement a complete privacy management framework see the OIPC website for Privacy Management Program at a Glance and Privacy Management Program: Getting Started, both available at: http://foipop.ns.ca/publicbodytools
[7] See the OIPC website for a PIA template for public bodies at: PIA Template.
[8] Essential FOIPOP policies include a privacy policy (describing collection, use & disclosure practices), breach management policy, records management policy and security policy. For more details on essential privacy policies review the privacy management program materials on the OIPC website.