PURPOSE
The following policy supports the protection of registrant information collected, used and disclosed by the Nova Scotia College of Pharmacists.

POLICY
Collection of Personal Information
For the purposes of this policy, personal information is information about an identifiable individual or information that can be readily processed to produce information about an identifiable individual. Aggregate information, which cannot be used to produce information about identifiable individuals, is not considered personal information.

The NSCP may collect the following information required about a registrant either directly from the registrant or indirectly from other regulatory authorities:
- Demographic Information - Name, date of birth, home address, home telephone number, home fax number, email address, gender, place of birth
- Education Information - Educational certificate(s) or university degree(s), Institution from which certificate(s) or degree(s) was granted, date of graduation, PEBC registration number, and any other educational certification with respect to the pharmacy profession
- Registration Status - Registration category, conditions on practice, competency information, complaint or discipline information, current or past registration with other jurisdiction or other licensing bodies
- Practice Information - Place of practice, address of employer, telephone, fax number and email address of employer
- Professional Competency - Continuing Education Programs completed, professional development activities undertaken, Continuing Competency/Quality Assurance assessments completed, etc.
- Other Information - Other information required for the registration process, including criminal record checks

Use of Personal Information
The NSCP may use information about registrants for the purpose of registering those individuals and to continue registering them, and to maintain registers and records in accordance with its mandate.

The NSCP may use registration information for conducting business that it is mandated to perform under provincial and federal legislation.

Disclosure of Personal Information
The Pharmacy Act requires the Registrar to comply with a request for verification of information contained in a register established under the Act. Registration information (a registrant’s registration status and practice site information, including work address, work phone number, work fax number and work email address) is not considered personal and confidential information. Consent is not necessary from the registrant for disclosure of such registration information.
Examples of such disclosure would include:
- Confirmation of registration to other licensing bodies
- Confirmation of registration to third party payers
- Confirmation of registration to drug wholesalers and manufacturers
- Confirmation of registration to any member of the public or press
- Confirmation of discipline procedures in accordance with legislation
- Any other purpose mandated by legislation or regulatory necessity
Consent
A registrant’s consent is not required for the collection, use and disclosure of personal information as required of the NSCP by legislation or regulation, as described above.

The NSCP will not disclose a registrant’s home address, home phone number, home fax number, or home email address without the registrant’s consent.

Openness and Access
The NSCP will provide information about the policies, procedures and practices related to its management of personal information about pharmacists. A registrant can access any personal information on file about himself or herself.

Accuracy and Integrity
The NSCP will take all reasonable steps to ensure that information on file is accurate, complete and as up to date as is necessary for the purpose for which it is to be used. A registrant has the right to question the accuracy of information on file concerning him or herself, and to request corrections to be made to such information.

Security
The NSCP will take reasonable steps to protect the registrant database.

Measures to ensure security of the NSCP’s database from unintentional disclosure and unauthorized access include a prescriptive process for the database vendor that includes:

- explicit and written authorization from the NSCP prior to the enabling of any public access to NSCP directories, and
- a process for monitoring that only those fields authorized for public access are coded as such in the database at any given time. Monitoring will be achieved by the following:
  (i) an itemization by the database vendor of the system areas capable of being accessed by the public
  (ii) a statement of policy by the NSCP regarding public access for those aforementioned areas
  (iii) an internal risk assessment by the database vendor and the NSCP related to possible unauthorized access to those aforementioned areas
  (iv) implementation by the database vendor of system settings to achieve the specifications regarding public access to meet the outcomes of (ii) and (iii)
  (v) training of the NSCP staff by the database vendor for the use of (iv)
  (vi) creation of an Operation Manual by the database vendor in relation to (iv)

Organizations that the NSCP authorizes to collect, store, maintain NSCP data and / or access the NSCP database will provide the NSCP with proof of Network Security and Breach of Privacy insurance, proof that the NSCP is named on that insurance certificate, and proof of the continuance of this insurance on an annual basis.

Privacy breaches will be handled in a manner consistent with applicable privacy legislation.