

Privacy and Confidentiality Policy

NorthBridge College (NBBT College)

Website: NBBTCollege.ca

Location: Moncton, New Brunswick, Canada

Compliance: Private Occupational Training Act (P-16.1), Regulation 84-207, and Applicable Privacy Legislation

Policy Title: Privacy and Confidentiality Policy

Approved by: Executive Director / College Administration

Effective Date: Aug.2026

Next Review Date: On or Before 31. Dec.2029

1. Background & Purpose

NorthBridge College (NBBT College) is a **private career college** operating under the **Private Occupational Training Act (P-16.1)** of New Brunswick, Canada. As a private institution, we recognize the importance of protecting the privacy and confidentiality of personal information collected from students, employees, and other individuals.

This Privacy and Confidentiality Policy governs the collection, use, disclosure, and protection of student and employee personal information. It supports compliance with privacy legislation and **Regulation 84-207, Section 15.1(3)**, which requires the protection of student record privacy as part of the College's obligation to maintain accurate student records while respecting individual privacy rights.

This policy is submitted as part of the College's registration application under **Regulation 84-207, Section 3.1(1)(a)(vii)**, which requires training organizations to submit policies that support student welfare, safety, and educational outcomes.

2. Scope

This policy applies to:

- All personal information collected, used, disclosed, or stored by NorthBridge College
 - All students (current, former, and prospective)
 - All employees (current and former staff, faculty, administrators, contractors)
 - All third parties who interact with the College (e.g., vendors, partners, visitors)
 - All formats of information (paper records, electronic records, digital files, audio/video recordings)
-

3. Principles of Fair Information Practices

NorthBridge College is committed to the following privacy principles, consistent with Canadian privacy legislation and best practices:

3.1 Accountability

- The College is responsible for all personal information under its control
- All staff and faculty are responsible for protecting personal information in their care

3.2 Identifying Purposes

- The purposes for collecting personal information will be identified before or at the time of collection
- Personal information will only be used for the purposes for which it was collected, or for compatible purposes

3.3 Consent

- Knowledge and consent are required for the collection, use, or disclosure of personal information, except where required or authorized by law
- Consent may be express (written or verbal) or implied, depending on the sensitivity of the information

3.4 Limiting Collection

- Personal information collected will be limited to what is necessary for the identified purposes
- Information will be collected by fair and lawful means

3.5 Limiting Use, Disclosure, and Retention

- Personal information will not be used or disclosed for purposes other than those for which it was collected, except with consent or as required by law
- Personal information will be retained only as long as necessary to fulfill the identified purposes
- Personal information will be disposed of securely when no longer needed

3.6 Accuracy

- Personal information will be as accurate, complete, and up-to-date as possible
- Individuals may request access to their personal information and request corrections

3.7 Safeguards

- Personal information will be protected by security safeguards appropriate to the sensitivity of the information
- Security measures include physical, technical, and administrative safeguards

3.8 Openness

- The College will make information about its privacy policies and practices readily available to individuals
- This policy and related procedures are available on the College website (NBBTCollege.ca) and upon request

3.9 Individual Access

- Individuals have the right to access their personal information held by the College
- Individuals may challenge the accuracy and completeness of their personal information and request corrections

4. Types of Personal Information Collected

4.1 Student Information

Admissions and Enrolment:

- Name, address, phone number, email address
- Date of birth, gender, citizenship
- Social Insurance Number (SIN) - for tax and financial aid purposes only
- Study permit information (for international students)
- Emergency contact information
- Previous education and transcripts
- Admission application and supporting documents

Academic Records:

- Program enrolment and course registration
- Attendance records
- Grades, transcripts, and academic standing
- Examination papers and results
- Assignments and assessment results

- Credentials awarded (diplomas, certificates)
- Academic accommodations and disability information
- Disciplinary records [Regulation 84-207, Section 15.1(1)(e)]laws.gnb+1

Financial Information:

- Tuition payment records
- Financial aid and student loan information
- Outstanding balances and collection records
- Receipts and financial correspondence

Additional Information:

- Photographs and video recordings (for identification, marketing, or security)
- Health and medical information (if required for program or accommodations)
- Criminal record check results (if required for program or work placement)
- Work placement evaluations and employer feedback
- Complaint or appeal records
- Graduation and employment outcome information

4.2 Employee Information**Personal and Contact Information:**

- Name, address, phone number, email address
- Date of birth, gender, citizenship
- Social Insurance Number (SIN) - for payroll and tax purposes
- Emergency contact information

Employment Records:

- Position, job description, and employment contract
- Salary, benefits, and payroll information
- Performance evaluations and reviews
- Training records and certifications
- Disciplinary records and grievances
- Termination or resignation records

Additional Information:

- Criminal record check results (if required for position)
- Medical information (if required for accommodations or workers' compensation)
- References and background check information

4.3 Third-Party Information**Vendors, Partners, and Visitors:**

- Business contact information (name, organization, phone, email)
- Contract and agreement information
- Visitor logs and access records
- Correspondence and communication records

5. Purposes for Collection and Use**5.1 Student Information**

Personal information is collected and used for the following purposes:

Educational Purposes:

- Processing applications for admission and enrolment

- Administering academic programs and courses
- Evaluating academic performance and progress
- Maintaining academic records and transcripts
- Awarding credentials (diplomas, certificates)
- Providing academic advising and student support services
- Arranging work placements, practicums, or field experiences
- Communicating with students about academic matters

Administrative Purposes:

- Verifying student identity
- Maintaining student records as required by Regulation 84-207, Section 15.1
- Complying with reporting requirements to the Minister under POTA
- Reporting to Immigration, Refugees and Citizenship Canada (IRCC) for international students
- Managing student accounts, tuition payments, and financial aid
- Collecting outstanding debts or referring to collection agencies
- Conducting surveys and research for institutional improvement

Safety and Security Purposes:

- Ensuring campus safety and security
- Responding to emergencies involving students
- Monitoring use of College facilities and technology
- Investigating student conduct violations or complaints

Marketing and Communications (with consent):

- Sending newsletters, updates, and event invitations
- Using photographs or testimonials in marketing materials
- Contacting alumni about College news and opportunities

5.2 Employee Information

Personal information is collected and used for the following purposes:

Employment Administration:

- Processing employment applications and hiring
- Administering employment contracts and benefits
- Processing payroll, taxes, and deductions
- Managing performance evaluations and promotions
- Maintaining employment records
- Providing training and professional development
- Administering terminations or resignations

Legal and Compliance:

- Complying with employment legislation and tax requirements
- Reporting to government agencies (e.g., CRA, Service Canada)
- Responding to legal proceedings or investigations

5.3 Third-Party Information

Personal information is collected and used for the following purposes:

- Managing vendor and partner relationships
- Processing contracts and agreements
- Maintaining visitor logs for security purposes

- Communicating about College business

6. Consent Requirements

6.1 Types of Consent

Express Consent:

- Written or verbal agreement to collection, use, or disclosure
- Required for sensitive information (e.g., health information, photographs for marketing)
- Examples: Signed consent forms, written agreements, verbal confirmation documented in file

Implied Consent:

- Consent inferred from an individual's actions or the circumstances
- Applies when the purpose is obvious and the individual voluntarily provides information
- Examples: Providing contact information for enrolment implies consent to use it for administrative communications

6.2 When Consent is Required

Consent is required for:

- Collection of personal information (except where required by law)
- Use of personal information for purposes beyond those for which it was collected
- Disclosure of personal information to third parties (except where required or authorized by law)
- Use of photographs or testimonials for marketing purposes
- Collection of sensitive information (e.g., health, disability, criminal records)

Consent is NOT required for:

- Information required by law (e.g., SIN for tax purposes, transcripts for regulatory reporting)
- Disclosure to the Minister under POTA for compliance monitoring
- Disclosure to IRCC for international student compliance
- Disclosure in emergency situations to protect health or safety
- Disclosure for legal proceedings (e.g., court order, subpoena)
- Information that is publicly available

6.3 Obtaining Consent

The College will:

- Inform individuals of the purposes for collection before or at the time of collection
- Provide clear and understandable consent forms
- Ensure consent is voluntary and not a condition of service (unless the information is necessary for the service)
- Allow individuals to withdraw consent at any time (subject to legal or contractual restrictions)
- Document consent in student or employee files

Students and employees may withdraw consent by:

- Submitting a written request to the Privacy Officer
- Understanding that withdrawal may limit the College's ability to provide certain services
- Acknowledging that some information collection is required by law and cannot be refused

7. Access to Personal Information

7.1 Right of Access

Under **Regulation 84-207, Section 15.1(2)**, students have the right to access their student records by submitting a request in writing.

Individuals have the right to:

- Request access to their personal information held by the College
- Receive a copy of their personal information (may be subject to fees)
- Understand how their information is being used and disclosed

7.2 How to Request Access**Requests must be submitted in writing to:**

Privacy Officer

NorthBridge College (NBBT College)

196 Robinson Street, 3rd Floor

Moncton, New Brunswick E1C 5C4

Email: [Insert Email]

Phone: [Insert Phone]

The request should include:

- Full name and contact information
- Student ID or employee ID (if applicable)
- Description of the information being requested
- Preferred format (viewing in person, email, or printed copy)
- Signature and date

7.3 Response Timeline

- The College will respond to access requests within **30 days** of receipt
- If additional time is needed, the individual will be notified in writing with reasons for the delay
- In most cases, responses will be provided within **10-15 business days**

7.4 Exceptions to Access**The College may deny or limit access to personal information in certain circumstances:**

- Information that contains references to other individuals (privacy of others must be protected)
- Information that is subject to solicitor-client privilege
- Information collected for an investigation or legal proceeding
- Information that could reasonably be expected to threaten the life or security of another individual
- Personal counselling notes (to protect therapeutic relationships)
- Information that is exempt from disclosure under applicable privacy legislation

If access is denied:

- The individual will be notified in writing with reasons for the denial
- The individual may file a complaint with the Privacy Officer or escalate to the appropriate privacy commissioner

7.5 Fees for Access

- **Viewing records in person:** No fee
- **Electronic copies (email):** No fee for current students/employees; \$25 for former students/employees
- **Printed copies:** \$0.50 per page (maximum \$50 per request)
- **Postage or courier:** At actual cost (if requested by individual)

Fees may be waived in cases of financial hardship at the discretion of the Privacy Officer.

8. Correction of Personal Information**8.1 Right to Request Correction**

Individuals have the right to:

- Request correction of inaccurate or incomplete personal information
- Challenge the accuracy and completeness of their information
- Request that corrected information be disclosed to third parties to whom the original information was disclosed

8.2 How to Request Correction**Requests must be submitted in writing to:**

Privacy Officer

NorthBridge College (NBBT College)

196 Robinson Street, 3rd

Moncton, New Brunswick E1C 5C4

Email: info@nbbtcollege.ca

Phone: +1-506-800-0851

The request should include:

- Full name and contact information
- Student ID or employee ID (if applicable)
- Description of the information to be corrected
- Explanation of why the information is inaccurate or incomplete
- Supporting documentation (if available)
- Signature and date

8.3 Review and Decision

- The College will review correction requests within **15 business days**
- If the request is approved, the information will be corrected promptly
- If the request is denied, the individual will be notified in writing with reasons for the denial

8.4 Notation of Disputed Information**If correction is denied but the individual continues to dispute the information:**

- A notation will be added to the record indicating the individual disputes the accuracy
- The individual's written statement of dispute will be attached to the record
- Future disclosures of the record will include the notation and statement of dispute

9. Disclosure to Third Parties**9.1 General Rule**

Personal information will not be disclosed to third parties without consent, except where required or authorized by law.

9.2 Permitted Disclosures (With Consent)**With individual consent, information may be disclosed to:**

- Prospective employers (e.g., for employment verification, reference checks)
- Other educational institutions (e.g., for transfer applications)
- Scholarship or bursary providers
- Family members or sponsors (for billing or communication purposes)
- Marketing partners (for promotional communications)
- Any other third party specified by the individual

9.3 Permitted Disclosures (Without Consent)**Information may be disclosed without consent in the following circumstances:**

Government and Regulatory Authorities:

- **Minister of Post-Secondary Education, Training and Labour** under POTA for compliance monitoring, reporting, or investigations
- **Immigration, Refugees and Citizenship Canada (IRCC)** for international student compliance (enrolment verification, completion reporting, status changes)
- **Canada Revenue Agency (CRA)** for tax reporting (e.g., tuition tax receipts)
- **Service Canada** for student loan and employment insurance reporting
- **Statistics Canada** or other government agencies for statistical purposes (with appropriate privacy protections)
- **New Brunswick Department of Post-Secondary Education, Training and Labour** for program registration and compliance

Legal and Safety:

- Law enforcement pursuant to a warrant, subpoena, or court order
- In emergency situations to protect the health or safety of the individual or others
- To legal counsel for the purpose of obtaining legal advice
- In connection with legal proceedings involving the College

Other Permitted Disclosures:

- Accrediting bodies or professional associations (limited to verification of credentials or program completion)
- Collection agencies or legal counsel for recovery of outstanding debts (limited to financial information)
- Researchers (with appropriate privacy protections and ethical approval)
- In the event of a privacy breach, to affected individuals and privacy commissioners as required by law

9.4 International Transfers**For international students or third-party service providers:**

- Personal information may be transferred to countries outside Canada for processing or storage (e.g., cloud-based student information systems, email providers)
- The College will ensure that appropriate safeguards are in place to protect information during international transfers
- Individuals will be informed if their information may be transferred outside Canada and may be subject to the laws of another country

9.5 Disclosure Logs**The College will maintain a record of disclosures:**

- Disclosures to third parties (with or without consent) will be documented
- Records will include: date of disclosure, recipient, information disclosed, and legal authority for disclosure
- Disclosure logs will be retained for **7 years** or as required by law

10. Data Security and Protection Measures**10.1 Physical Safeguards****The College will implement physical security measures:**

- **Secure Facilities:** Buildings are locked after hours; access is restricted to authorized personnel
- **Locked Storage:** Paper records are stored in locked filing cabinets or secure rooms

- **Access Controls:** Key cards or keys are issued only to authorized staff and faculty
- **Visitor Management:** All visitors must sign in and wear visitor badges; visitors are escorted in restricted areas
- **Secure Disposal:** Shredding bins are provided for confidential documents; records are shredded before disposal

10.2 Technical Safeguards

The College will implement technical security measures:

- **Password Protection:** All computer systems and databases require strong passwords
- **Encryption:** Sensitive data is encrypted during transmission and storage
- **Access Controls:** User accounts and permissions are assigned based on role and need-to-know
- **Firewalls and Antivirus:** Computer systems are protected by firewalls and antivirus software
- **Regular Updates:** Software and security patches are updated regularly
- **Backup Systems:** Data is backed up regularly to prevent loss from system failures
- **Secure Networks:** Wi-Fi networks are encrypted and require authentication
- **Multi-Factor Authentication:** Required for sensitive systems (e.g., student information systems, financial systems)

10.3 Administrative Safeguards

The College will implement administrative security measures:

- **Privacy Training:** All staff and faculty receive privacy and security training upon hire and annually
- **Confidentiality Agreements:** Staff and faculty sign confidentiality agreements as a condition of employment
- **Access Reviews:** User access rights are reviewed periodically and updated when roles change
- **Incident Response:** Privacy breach response procedures are in place and tested regularly
- **Vendor Management:** Third-party vendors are required to sign data protection agreements
- **Clean Desk Policy:** Confidential information is not left unattended on desks or in public areas
- **Secure Transmission:** Sensitive information is transmitted securely (e.g., encrypted email, secure file transfer)

10.4 Security of Student Records

Under **Regulation 84-207, Section 15.1(3)**, the College is required to protect the privacy of student records while maintaining them for the required retention period.

Student records are protected by:

- Storing active records in secure, access-controlled areas
- Limiting access to authorized staff with a legitimate need to know
- Using password-protected and encrypted electronic systems
- Regularly reviewing and updating security measures
- Conducting periodic security audits and risk assessments

11. Privacy Breach Response

11.1 Definition of Privacy Breach

A **privacy breach** occurs when personal information is:

- Accessed, collected, used, or disclosed without authorization
- Lost, stolen, or destroyed
- Altered or destroyed without authorization
- Disclosed in violation of this policy or applicable privacy legislation

Examples:

- Lost or stolen laptop or USB drive containing personal information
- Email sent to wrong recipient containing sensitive information
- Unauthorized access to computer systems or databases (hacking)
- Paper records lost or stolen
- Inappropriate disclosure by staff or faculty (e.g., discussing student information in public)

11.2 Breach Response Procedures**Step 1: Containment**

- Immediately contain the breach (e.g., recover lost documents, change passwords, disable compromised accounts)
- Prevent further unauthorized access or disclosure

Step 2: Assessment

- Assess the nature and scope of the breach
- Determine what information was affected and how many individuals are impacted
- Evaluate the risk of harm to affected individuals (e.g., identity theft, financial loss, reputational harm)
- Identify the cause of the breach and responsible parties

Step 3: Notification

- **Notify Affected Individuals:** Notify individuals whose personal information was breached, if there is a real risk of significant harm
- **Notify Privacy Commissioner:** Report the breach to the appropriate privacy commissioner (e.g., Office of the Privacy Commissioner of Canada, provincial privacy commissioner) if required by law
- **Notify the Minister:** Report serious breaches to the Minister of Post-Secondary Education, Training and Labour under POTA
- **Notify Law Enforcement:** Report breaches involving criminal activity (e.g., theft, hacking) to police

Step 4: Mitigation

- Take steps to mitigate harm to affected individuals (e.g., offer credit monitoring, provide support services)
- Implement corrective actions to prevent similar breaches (e.g., additional training, improved security measures)

Step 5: Documentation and Review

- Document the breach, response actions, and outcomes
- Review the incident to identify lessons learned and areas for improvement
- Update policies and procedures as necessary

11.3 Breach Notification to Individuals**When individuals must be notified:**

- If there is a real risk of significant harm (e.g., identity theft, financial loss, reputational harm, physical harm)
- Notification will be provided as soon as feasible after the breach is discovered
- Notification will include:
 - Description of the breach and what information was affected
 - Steps the College has taken to mitigate harm
 - Steps individuals can take to protect themselves (e.g., monitor credit reports, change passwords)
 - Contact information for questions or concerns

Methods of Notification:

- Direct communication (e.g., phone call, email, letter)
- Public notice (e.g., website, media) if direct communication is not feasible or would cause further harm

11.4 Breach Reporting to Regulatory Authorities**The College will report breaches to:**

- **Office of the Privacy Commissioner of Canada:** For breaches involving federal private sector organizations or interprovincial matters
- **New Brunswick Office of the Information and Privacy Commissioner:** For breaches involving provincial public sector or applicable private sector organizations
- **Minister of Post-Secondary Education, Training and Labour:** For breaches affecting students under POTA
- **Law Enforcement:** For breaches involving criminal activity (e.g., theft, fraud, hacking)

12. Retention and Disposal of Personal Information**12.1 Retention Periods**

Personal information will be retained only as long as necessary to fulfill the purposes for which it was collected, or as required by law.

Student Records:

Record Type	Retention Period	Regulatory Basis
Credentials Awarded (diplomas, certificates)	50 years after date of registration	Regulation 84-207, Section 15.1(4)
Transcripts	50 years after date of registration	Regulation 84-207, Section 15.1(4)
Student Contract	7 years after program completion or withdrawal	Regulation 84-207, Section 15.1
Examination Papers and Results	7 years after program completion or withdrawal	Regulation 84-207, Section 15.1(1)(b)
Assignments and Results	7 years after program completion or withdrawal	Regulation 84-207, Section 15.1(1)(c)
Proof of Attendance	7 years after program completion or withdrawal	Regulation 84-207, Section 15.1(1)(d)
Record of Disciplinary Action	7 years after program completion or withdrawal	Regulation 84-207, Section 15.1(1)(e)
Financial Records	7 years after final transaction	Canada Revenue Agency requirements
Complaint or Appeal Records	7 years after resolution	Student Complaint Policy
International Student Records (study permit, IRCC reporting)	7 years after program completion or permit expiry	IRCC requirements

Employee Records:

Record Type	Retention Period	Regulatory Basis
Employment Records (contracts, payroll, benefits)	7 years after termination	Employment Standards and CRA requirements
Performance Evaluations	7 years after termination	Best practices
Training Records	7 years after completion or departure	Occupational Health and Safety requirements
Disciplinary Records	7 years after termination	Best practices

Third-Party Records:

Record Type	Retention Period	Regulatory Basis
Vendor and Partner Contracts	7 years after contract expiration	Legal and business requirements
Visitor Logs	1 year	Security purposes

12.2 Secure Disposal

When personal information is no longer needed:

Paper Records:

- Shredded using cross-cut shredders
- Placed in secure shredding bins for professional disposal
- Documentation of disposal (date, type of records, person responsible)

Electronic Records:

- Permanently deleted from all systems and backups
- Hard drives or storage devices are wiped or physically destroyed
- Documentation of disposal (date, type of records, method, person responsible)

Other Media:

- Microfilm, microfiche, or other media are destroyed securely
- Documentation of disposal is maintained

12.3 Disposal Logs

The College will maintain a record of disposals:

- Date of disposal
- Type of information disposed
- Method of disposal
- Person responsible for disposal

Disposal logs will be retained for **7 years** or as required by law.

13. Privacy Officer**13.1 Designation**

NorthBridge College has designated a **Privacy Officer** responsible for:

- Overseeing compliance with this policy and applicable privacy legislation
- Receiving and responding to privacy inquiries, complaints, and breach reports
- Conducting privacy impact assessments for new programs or systems
- Providing privacy training and guidance to staff and faculty
- Reviewing and updating this policy annually
- Serving as the primary contact for privacy commissioners and regulatory authorities

13.2 Contact Information

Privacy Officer:

NorthBridge College (NBBT College)

Moncton, New Brunswick

Email: info@nbbtcollege.ca

13.3 Responsibilities

The Privacy Officer will:

- Monitor compliance with this policy and applicable privacy legislation
- Investigate privacy complaints and breaches
- Provide guidance on privacy matters to staff, faculty, and students
- Conduct privacy impact assessments for new initiatives
- Report to the Executive Director on privacy compliance and issues
- Maintain documentation of privacy training, complaints, and breaches
- Liaise with privacy commissioners and regulatory authorities

14. Privacy Training and Awareness**14.1 Training Requirements**

All staff and faculty must complete privacy training:

- **New Employees:** Privacy training during orientation (within first 30 days of employment)
- **Annual Refresher:** Annual privacy and security awareness training
- **Role-Specific Training:** Additional training for staff with access to sensitive information (e.g., admissions, student records, payroll)

14.2 Training Content

Privacy training will cover:

- This Privacy and Confidentiality Policy
- Applicable privacy legislation and principles
- Types of personal information collected and purposes
- Consent requirements and procedures
- Access and correction procedures
- Data security and protection measures
- Privacy breach response procedures
- Consequences of non-compliance

14.3 Training Records

The College will maintain:

- Records of all privacy training completed by staff and faculty
- Training materials and resources
- Assessment results (if applicable)

Training records will be retained for **7 years** or as required by law.

15. Complaints and Inquiries**15.1 Filing a Complaint**

Individuals who believe their privacy rights have been violated may file a complaint:

Submit complaints in writing to:

Privacy Officer
NorthBridge College (NBBT College)
196 Robinson Street, 3rd Floor
Moncton, New Brunswick E1C 5C4
Email: [Insert Email]
Phone: [Insert Phone]

The complaint should include:

- Full name and contact information
- Description of the privacy concern or violation
- Dates and details of the incident(s)
- Any supporting documentation
- Signature and date

15.2 Complaint Investigation

- The Privacy Officer will acknowledge receipt of the complaint within **5 business days**
- The Privacy Officer will investigate the complaint and respond within **30 days**
- If additional time is needed, the individual will be notified in writing with reasons for the delay
- The investigation may include:
 - Review of relevant documents and records
 - Interviews with staff, faculty, or other individuals
 - Consultation with legal counsel or privacy commissioners (if necessary)

15.3 Complaint Resolution

The Privacy Officer will:

- Notify the individual of the outcome in writing
- If a violation is found, take corrective action (e.g., policy changes, training, disciplinary action)
- Provide information on further recourse (e.g., filing a complaint with privacy commissioner)

15.4 Escalation to Privacy Commissioner

If the individual is not satisfied with the College's response:

They may file a complaint with the appropriate privacy commissioner:

- **Office of the Privacy Commissioner of Canada:**
Website: www.priv.gc.ca
Phone: 1-800-282-1376
- **Ombud New Brunswick**
Website: [Make A Complaint](#)
Phone: 1-888-465-1100

16. Third-Party Service Providers

16.1 Vendor Management

The College may use third-party service providers to process or store personal information:

Examples:

- Student information systems (e.g., cloud-based platforms)
- Email and communication services (e.g., Gmail, Microsoft 365)
- Payment processing services (e.g., credit card processors)
- Data backup and storage services
- Marketing and communication platforms

16.2 Data Protection Agreements

The College will require third-party vendors to:

- Sign data protection agreements or contracts
- Comply with this Privacy and Confidentiality Policy
- Implement appropriate security safeguards
- Use personal information only for specified purposes
- Not disclose personal information to other parties without authorization
- Notify the College of any privacy breaches
- Return or destroy personal information when the contract ends

16.3 International Service Providers

If personal information is transferred to service providers outside Canada:

- The College will ensure appropriate safeguards are in place (e.g., contractual protections, encryption)
- Individuals will be informed that their information may be processed in another country and may be subject to the laws of that country
- The College will assess the privacy laws and practices of the country where information is processed

17. Policy Review and Updates

17.1 Annual Review

This Privacy and Confidentiality Policy will be reviewed **annually** by:

- Privacy Officer
- Executive Director
- Legal counsel (if applicable)

17.2 Review Triggers

The policy may be reviewed more frequently if:

- There are changes to privacy legislation or regulations
- Privacy breaches or incidents occur
- New programs or systems are implemented
- Feedback from students, staff, or privacy commissioners indicates need for improvement

17.3 Communication of Changes

When the policy is updated:

- Changes will be communicated to all students and employees
- The updated policy will be posted on the College website (NBBTCollege.ca)
- Training will be provided to staff and faculty on significant changes
- Individuals will be notified of their right to access and correct their personal information

18. Related Policies

This Privacy and Confidentiality Policy should be read in conjunction with the following NorthBridge College (NBBT College) policies:

Policy Name	Relationship to Privacy
Student Records Policy	Defines student record-keeping requirements and access procedures

Policy Name	Relationship to Privacy
Health and Safety Policy	Protects health and medical information collected for safety purposes
Information Technology and Acceptable Use Policy	Governs use of technology and protection of electronic information
Student Code of Conduct	Prohibits unauthorized access or disclosure of personal information
Sexual Violence and Misconduct Policy	Protects confidentiality of survivors and respondents
Student Complaint Submission and Resolution Policy	Protects privacy of complainants and respondents
Employee Confidentiality Agreement	Requires staff and faculty to protect personal information

19. Legislative Compliance

This policy is developed in compliance with:

- **Private Occupational Training Act (P-16.1)**, New Brunswick, particularly:
 - Section 15.1: Student record-keeping and privacy requirements
 - 2024 Legislative Amendments: Enhanced student protections and privacy
- **Regulation 84-207 (General)**, New Brunswick, particularly:
 - Section 3.1(1)(a)(vii): Requirement to submit policies supporting student welfare and safety
 - Section 15.1(2): Student right of access to records
 - Section 15.1(3): Protection of student record privacy
 - Section 15.1(4): Retention of credentials and transcripts for 50 years
- **Personal Information Protection and Electronic Documents Act (PIPEDA)**, Canada (if applicable to private career colleges)
- **New Brunswick Personal Information Protection Act** (if applicable)
- **Freedom of Information and Protection of Privacy Act**, New Brunswick (for reference)
- **Canada Anti-Spam Legislation (CASL)** (for electronic communications)

Note: As a private career college, NorthBridge College may be subject to federal privacy legislation (PIPEDA) or provincial privacy legislation depending on the nature of operations and applicable laws. The College should consult with legal counsel to determine specific privacy obligations.

20. Definitions

Term	Definition
Personal Information	Information about an identifiable individual (e.g., name, address, student ID, grades, health information)
Privacy Breach	Unauthorized access, collection, use, disclosure, loss, or destruction of personal information
Consent	Voluntary agreement to the collection, use, or disclosure of personal information (may be express or implied)
Privacy Officer	The designated individual responsible for overseeing compliance with this policy and privacy legislation

Term	Definition
Third Party	Any individual or organization other than the individual, the College, or the College's agents
Express Consent	Explicit agreement given in writing, verbally, or electronically
Implied Consent	Consent inferred from an individual's actions or the circumstances
De-identified Information	Information that has been stripped of identifying elements and cannot reasonably be linked to an individual
Minister	The Minister of Post-Secondary Education, Training and Labour for the Province of New Brunswick

21. Important Note for NorthBridge College

NorthBridge College (NBBT College) is a private career college operating under the Private Occupational Training Act of New Brunswick, Canada. We are not a publicly funded or community college.

As a private institution, we have the authority and responsibility to:

- Establish comprehensive privacy policies and procedures within the framework of POTA and applicable privacy legislation
- Collect, use, and disclose personal information only for legitimate purposes and with appropriate consent
- Protect student and employee personal information with appropriate security safeguards
- Maintain accurate student records as required by Regulation 84-207, Section 15.1 while respecting privacy
- Report privacy breaches to the Minister and privacy commissioners as required under POTA and privacy legislation
- Provide individuals with access to their personal information and the right to request corrections
- Comply with Ministerial orders and remedial actions directed under Section 6.8 of POTA

This policy reflects our commitment to protecting the privacy and confidentiality of personal information while maintaining the integrity and standards of NorthBridge College as a private career college in New Brunswick, Canada.

22. Contact Information

For questions regarding this policy or to submit privacy requests, complaints, or breach reports:

Privacy Officer:

NorthBridge College (NBBT College)

Moncton, New Brunswick, Canada

Website: NBBTCollege.ca

Email: info@nbbtcollege.ca

Phone: +1-506-800-0851

For External Privacy Complaints:

Office of the Privacy Commissioner of Canada:

Website: www.priv.gc.ca

Phone: 1-800-282-1376

Email: info@priv.gc.ca

Ombud New Brunswick

Website: <https://ombudnb.ca/make-a-complaint/>

Phone: 1-888-465-1100

Email: ombud@ombudnb.ca

For Complaints Under POTA:

Private Occupational Training Branch

Department of Post-Secondary Education, Training and Labour

Government of New Brunswick

Email: LFPSP-POTA@gnb.ca

Phone: (506) 453-2597

Student Complaint Form: <https://www2.gnb.ca/content/dam/gnb/Departments/petl-epft/PDF/POTA/student-complaint-form.pdf>