
Information Security Data Classification Guidelines

Purpose

The purpose of data classification is to ensure that all NBCC information assets are identified, classified, and handled in a consistent and appropriate manner based on their sensitivity, value, and risk. Data classification establishes clear requirements for the protection, handling, distribution, and disposal of information to safeguard confidentiality, integrity, and availability. This approach enables staff to manage and protect information responsibly throughout its lifecycle.

Scope

This guideline applies to all NBCC information assets, regardless of format or medium, including but not limited to electronic data, paper records, microfilm, emails, databases, reports, removable media, and cloud-based information systems. It applies to all NBCC employees, contractors, consultants, students, and third parties who create, capture, access, process, store, transmit, and/or apply final disposition of NBCC information assets.

The requirements defined in this guideline apply throughout the entire information lifecycle, from capture and use to storage, distribution, and final disposition.

Definitions

Clean Desk Policy: Clearing the desk of all documents at the end of each day, disposing of them securely or placing them in appropriate storage.

Encryption: The rendering of electronic data or documents unintelligible to unauthorized users. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Tacit Knowledge: Knowledge, experience, or institutional history held by an individual that has not been captured or recorded in any document, system, or repository. Because it exists only in a person's memory, tacit knowledge is not classified until it is captured. The moment it is written, typed, or spoken into any system, including an AI tool, it must be classified as if it were being documented for the first time.

Implementation

Authors and authorized users are responsible for accurately classifying information assets at the time of capture. Each asset must be clearly labeled and handled in accordance with the requirements set out in these guidelines throughout its entire lifecycle.

Basic Principles

When information contains elements of differing sensitivity, it must be classified according to the highest applicable level. For example, if a document includes both public and confidential information, the entire document should be classified as confidential. If there is any uncertainty regarding the classification, the information should default to the next highest level of sensitivity.

It is important to note that the classification and sensitivity of information can change depending on context. Data that may typically be considered less sensitive could become restricted when combined with other details. For instance, while an individual's name alone may be confidential, linking it with their Social Insurance Number, residential address, salary, and payroll deductions on a T4 form elevates the classification to restricted.

Using Data Classifications

The guidelines and accompanying tables provide descriptions of the various data classification levels, along with suggested handling practices. While the examples are not exhaustive, they are intended to assist members of the NBCC community in applying appropriate data management practices.

Other Related Documents

Data classification security and handling practices should be viewed in the context of the following related legislation, policies and other standards applicable to NBCC:

- Records and Information Management (5306)
- Information Security Policy (2808)
- Acceptable Use of Technology Resources (2808.4750)
- Privacy and Access to Information (4139)
- Right to Information and Protection of Privacy Act (RTIPPA)
- Personal Health Information Privacy and Access Act (PHIPAA)
- Personal Information Protection and Electronic Documents Act (PIPEDA) (as a guiding principle)

List of Tables

- Table 1: Data Classification Guidelines
- Table 2: Access Guidelines
- Table 3: Data Residency Guidelines
- Table 4: AI Tool Data Handling Guidelines
- Table 5: Storage Classification Guidelines
- Table 6: Labelling and Visual Identity Guidelines
- Table 7: Transmission Guidelines
- Table 8: Printing and Copying Guidelines
- Table 9: Disposition Guidelines

Table 1: Data Classification Guidelines

	Definition	Examples of Information	Examples of Risk Impacts
Restricted	Highly sensitive information intended only for specifically authorized users because it requires the strongest safeguards and strict control over access, use, and distribution.	• Closed sessions of SET/Board of Governors • Some security response plans • Some IT technical data about networks and systems • Locations of hazardous material storage • Passwords • Personal health information • Social insurance number • Banking and credit card information • Personal information related to children • Payroll information • Employee work performance information • Biometric data such as fingerprints • Tax information	• Serious harm to individuals, including fraud or identity theft • Major damage to the College's reputation and trust • Significant financial loss, penalties, or legal consequences • Risk to personal safety or wellbeing • Severe impact on college operations, strategy, or partnerships
Confidential	Sensitive information intended for use by those who are authorized users for a very specific business purpose such as confidential College business, proprietary research, or personal/private information.	• Briefing notes • Employment records • Admissions Applications • Personal identifiable information (some personal information is classified as highly confidential) • Intellectual property • Student or employee number • Contracts and other legal documents and materials • Internal audit reports and working papers • Drafts of strategic plans, annual reports and financial statements • Pension information • Employment competitions and searches • Exams, assignments, tests	• Loss of trust or damage to the College's reputation • Likely to attract media or public attention • Harm to personal privacy • Risk of financial loss or legal issues • Exposure could affect funding, partnerships, or competitive position • Information being changed or lost would cause significant disruption

	Definition	Examples of Information	Examples of Risk Impacts
Operational	Information intended for use by authorized users conducting College business, including employees, applicants, students, alumni, partners, government bodies.	• Risk Register • Employee Code of Conduct • Seat capacity report • Administration procedures, operational guides, planning documents • Non-public vendor or service provider contracts • Internal memoranda, emails and other documents • Non-public reports, budgets, plans and financial information • Internal communications regarding projects, etc. • Detailed floor plans, access codes, etc. • Drafts of public information	• Some disruption to college operations if the information is unavailable • Low risk to people's safety • Small impact on staff workload • Low legal or financial risk • Some risk to trust or credibility if the information is changed or shared improperly • May attract limited media attention if exposed.
Public	Information approved for distribution to the public by the information owner.	• Academic Calendar • Policies & By-Laws • Published reports to the community • Publicly posted news releases • Published marketing information • Course/program information • Job postings • Published annual reports • Financial statements	• Little or no impact on people or the College • Minor inconvenience if the information is unavailable • Low risk to the College's reputation if the information is changed (for example, a public webpage is altered) • If the information is lost, changed, or unavailable, it would not cause harm.

Table 2: Access Guidelines

Below are access expectations by data classification level. Controls become progressively stricter as sensitivity increases. Public information has no access restrictions, while Internal and Confidential information must be limited to authorized functions, groups, or roles using least privilege and need-to-know principles, with access removed as soon as it is no longer required. Restricted information requires the tightest controls, limiting access to specific named individuals or positions and emphasizing prompt revocation when roles change or employment ends.

	Restricted	Confidential	Operational	Public
Access	- Access is limited to specific named individuals or positions. - Principles of least privilege and need-to-know must be applied. - Access must be immediately revoked when users leave the College, custodial unit, change position and/or no longer require the information	- Access is limited to individuals in a specific function, group, or role. - Principles of least privilege and need-to-know must be applied. - Access must be immediately revoked when users leave the College, custodial unit, change position and/or no longer require the information.	- Access is limited to individuals in a specific function, group, or role. - Principles of least privilege and need-to-know must be applied. - Access must be immediately revoked when users leave the College, department/school, changes position and/or no longer requires the information.	No access restrictions

Table 3: Data Residency Guidelines

This table provides guidance on where data may be stored and processed, based on the data classification level and applicable provincial/federal requirements. Where a service's actual storage/processing location is unknown, treat it as outside Canada until confirmed by IT and the service provider. Use of any external/cloud service must undergo an appropriate security assessment and approval by IT Security prior to use.

Topic	Restricted	Confidential	Operational	Public
Residency Expectation	Canada only. Do not store/process outside Canada.	Canada only. Do not store/process outside Canada.	Canada by default. If storage/processing in Canada is not possible, other locations may be used only with documented justification and prior approval by IT.	No residency restriction, provided information is approved for public release.
Allowed Storage Locations	Canada (including Canadian cloud regions) only.	Canada (including Canadian cloud regions) only.	Canada by default. If storage/processing in Canada is not possible, EU locations may be used only with (1) access limited to authorized College users, (2) an appropriate security assessment, and (3) prior approval by IT.	Any location.
Cross-Border Access / Support	Not permitted.	Not permitted.	Permitted where access remains limited to authorized College users and is supported by IT-approved controls (e.g., role-based access, logging). If support or access would occur outside Canada, it is permitted only if the service is approved for EU processing and has prior approval by IT.	Permitted.
Examples of Suitable Platforms	NBCC-approved systems hosted in Canada with strict access controls.	NBCC-approved systems hosted in Canada; encrypted storage; controlled access.	NBCC-managed services hosted in Canada by default (e.g., NBCC-managed Microsoft 365). If a service cannot be hosted/processed in Canada, it may be used only if it is hosted/processed in the EU and has prior approval by IT.	NBCC public website(s).

Note: “Canada” means data is stored in Canadian facilities/regions and is not replicated to or processed in other countries (including for backup, failover, telemetry (logs/metrics/diagnostic data), or support) unless the information is classified as Public or Internal and an approved business arrangement exists. For **Confidential** and **Restricted** information, storage and processing must remain in Canada and cross-border access is not permitted.

Table 4: AI Tool Data Handling Guidelines

This table applies the classification levels in Table 1 specifically to AI tools, including chat assistants, copilots, and AI agents. Where an AI tool is not listed here, apply the most restrictive applicable row until the tool has been added to the Approved Platform Guide and this table is updated.

Restricted	Confidential	Operational	Public
Not permitted. Restricted information must not be entered into an AI tool, as these tools may process, store, or expose information.	Not permitted. Confidential information must not be entered into an AI tool, as these tools may process, store, or expose information.	Information classified as Operational may be entered into NBCC-approved AI tools.	No restrictions.

AI Considerations: Tacit Knowledge and Voice/Audio Input

Tacit knowledge, institutional history, unwritten procedures, or experience that exists only in an individual's memory, is not itself classified under Table 1, since it has not been captured in any recorded form. However, once tacit knowledge is typed, dictated, or otherwise entered into an AI tool, it becomes a data asset like any other and must be classified based on its content, not its source. Before sharing institutional knowledge with an AI tool, in writing or verbally, staff should ask the same question they would ask before typing it into any other system: what classification would this receive if it were being documented for the first time?

AI tools that accept voice or audio input (including dictation, voice notes, and meeting transcription) capture more than the words spoken. They may also capture the speaker's voice itself, a biometric and personally identifying characteristic in its own right, separate from the content of what was said. Voice input should be evaluated on two dimensions:

1. the classification of the content being spoken, per Table 9 above, and
2. the fact that voice data may itself warrant Restricted-level handling given its biometric nature (see Table 1, "Biometric data such as fingerprints"), regardless of how innocuous the spoken content is.

This is a developing area of guidance and will be revisited as AI voice tools become more prevalent at NBCC.

Table 5: Storage Classification Guidelines

Depending on the classification, information will need different types of storage requirements to ensure the confidentiality, integrity, accessibility, and value of the information are protected.

	Restricted	Confidential	Operational	Public
Storage Printed Materials	- Store in a secure manner. For example, within a file cabinet, safe or drawer that is always locked. Ensure room is locked, preferably in an alarmed area. - Clean desk policy.	- Store in a secure manner, i.e., within a file cabinet or drawer that is locked in non-working hours. Ensure room is locked during non-working hours. - Clean desk policy.	- Store in secure location (e.g. locked office, locked file room, locked file cabinet or desk drawer that is locked during non-working hours). - Clean desk policy	No special precautions are required.
Storage Removable Media	- Not permitted unless encrypted. - Personal information and personal health information are prohibited unless encrypted. - Store in a secure manner, i.e., within a file cabinet, safe or drawer that is always locked. Ensure room is locked, preferably in an alarmed area.	- Not permitted unless encrypted. - Personal information is prohibited unless encrypted. - Store in a secure manner, i.e., within a file cabinet, safe or drawer that is locked at all times. Ensure room is locked during non-working hours.	- No special precautions are required. - Store in secure location (e.g. locked office, locked file room, locked file cabinet or desk drawer that is locked during non-working hours). - Clean desk policy	No special precautions are required.
SharePoint (IT Administered)	Ensure only authorized users have access to the file(s); be aware of all members of the SharePoint site to ensure they are authorized to have access to the information.	Ensure only authorized users have access to the file(s); be aware of all members of the SharePoint site to ensure they are authorized to have access to the information.	Ensure only authorized users have access to the file(s); be aware of all members of the SharePoint site to ensure they are authorized to have access to the information.	No special precautions are required.
Self-Serve SharePoint	Not permitted.	Ensure only authorized users have access to the file(s); be aware of all members of the SharePoint site to ensure they are authorized to have access to the information.	Ensure only authorized users have access to the file(s); be aware of all members of the SharePoint site to ensure they are authorized to have access to the information.	No special precautions are required.
OneDrive	Not permitted.	Ensure only authorized users have access to the file(s).	Ensure only authorized users have access to the file(s).	No special precautions are required.

	Restricted	Confidential	Operational	Public
Network Drive	Ensure only authorized users have access to the file(s); be aware of who may have access to the network drive folders/files to ensure they are authorized to have access to the information.	Ensure only authorized users have access to the file(s); be aware of who may have access to the network drive folders/files to ensure they are authorized to have access to the information.	Ensure only authorized users have access to the file(s); be aware of who may have access to the network drive folders/files to ensure they are authorized to have access to the information.	No special precautions are required.
Personal Cloud	Not permitted.	Not permitted.	Not permitted.	No special precautions are required.

Table 6: Labelling and Visual Identity Guidelines

The actual labelling procedure will vary depending on the medium in which the information is stored. Below are sample labelling methods.

Type	Guideline
Printed Documents & Materials	Rubber ink-stamps for each classification level may be needed to mark hardcopy documents received from outside NBCC.
Email	The classification shall be tagged in the email automatically when the sensitivity is selected.
Fax	Identify the classification in the subject line on the fax cover sheet.
Digital Content	- This will automatically be applied when the sensitivity is selected: - Data classification identified in document metadata. - The classification should appear on every page, including the cover page (the classification will be in the header/footer or by use of a watermark).
Other Media	The data classification may be identified on adhesive labels applied to other media such as CD/DVDs, USB memory sticks, etc.

Table 7: Transmission Guidelines

	Restricted	Confidential	Operational	Public
Conversation/ Meetings	Enclosed meeting area. Discussion in public areas prohibited.	Private setting / lowered voices. Avoid public areas such as elevators, hallways, cafeterias.	Ensure you are not overheard.	No special precautions are required.
Telephone	- Avoid proximity to unauthorized listeners. - Speakerphone discouraged unless in enclosed area. - Preferably discussed in an enclosed, secured area. - Ensure you are not overheard.	- Avoid proximity to unauthorized listeners. - Speakerphone in enclosed area. - Ensure you are not overheard.	Ensure you are not overheard.	No special precautions are required.
Voicemail	Only leave name and contact details for callback.	- Only leave name and contact details for callback. - For personal information, leave only name and contact details for callback unless the individual has given prior consent to leave a message.	- Leave brief details. - Try to ensure you are not overheard while leaving the message.	No special precautions are required.
College Mail	- Enclose in double envelope with the inner envelope sealed and labelled "Restricted" on both front and back. Outer inter-office envelope, sealed with the recipient's name. - Notify the recipient in advance.	Enclose in double envelope sealed and labelled "Confidential" and the outer inter-office envelope sealed with the recipient's name.	Enclosed in sealed inter-office envelope.	No special precautions are required.
Outside Mail	- Use authorized bonded courier service or registered mail only. - Enclosed in double envelope. Seal the inner envelope, label "Restricted" on both the front and back and place recipient's name and address on the front. - Outer envelope is sealed, displaying the recipient's name/address with the return address clearly displayed.	- For personal information, use authorized courier services or registered mail. Only use regular mail if the individual has provided consent; otherwise use authorized courier service or registered mail. - Mark "Confidential" with the return address clearly displayed.	Use regular mail.	No special precautions are required.

	Restricted	Confidential	Operational	Public
Fax	- Avoid faxing if possible. If use of fax is required, fax only information that needs to be transmitted immediately. - Telephone before faxing to ensure recipient is waiting to receive the fax. - A fax coversheet is required labelled "Restricted"; identify both the sender and intended receiver on the coversheet. - Call to confirm successful transmission. - Check that the receiver's number is correct; verify in the machine's display window that number is keyed in correctly.	- Avoid faxing if possible. If use of fax is required, fax only information that needs to be transmitted immediately. - Telephone before faxing to ensure recipient is waiting to receive the fax. - A fax coversheet is required labelled "Confidential"; identify both the sender and intended receiver on the coversheet. - Call to confirm successful transmission. - Check that the receiver's number is correct; verify in the machine's display window that number is keyed in correctly.	- A fax coversheet is required. Identify both the sender and intended receiver on the coversheet. - Check that the receiver's number is correct; verify in the machine's display window that number is keyed in correctly.	- A fax coversheet is required. Identify both the sender and intended receiver on the coversheet. - Check that the receiver's number is correct; verify in the machine's display window that number is keyed in correctly.
Email	- Encrypted email strongly recommended; data may be masked instead of encrypting. See restrictions on emailing SIN and credit card information below. - Emailing credit card information & number is not permitted. - Emailing SIN is not permitted unless transmission by email is necessary and only to a government body or regulator; email must be encrypted. - Use NBCC email. - Double-check the email address before sending.	- Encrypted email strongly recommended; data may be masked instead of encrypting. - Use NBCC email. - Double-check the email address before sending it. - Emailing someone's own personal information to them is strongly discouraged unless the individual has given prior consent.	- Use NBCC email. - Double-check the email address before sending.	- No special precautions are required, - Use NBCC Email if you are conducting NBCC business.
MS Teams in Team / Channel	Not permitted. Use alternate method for transmitting information such as encrypted email.	Ensure all Team members are authorized to have access to the information.	Ensure all Team members are authorized to have access to the information.	No special precautions are required.
MS Teams Chat	Not permitted. Use alternate methods for transmitting information such as encrypted email.	Not permitted. Use alternate method for transmitting information such as encrypted email.	Double-check recipient address to ensure sending to correct individual.	No special precautions are required.

	Restricted	Confidential	Operational	Public
Other Messaging Apps Including Text (SMS)	Not permitted. Transmission by instant messaging, text message/SMS/MMS, instant messaging is not permitted as it is not a secure means to transmit information and can easily be intercepted.	Not permitted. Transmission by instant messaging, text message (SMS/MMS), instant messaging is not permitted as it is not a secure means to transmit information and can easily be intercepted.	Not permitted. Transmission by instant messaging, text message (SMS/MMS), instant messaging is not permitted as it is not a secure means to transmit information and can easily be intercepted.	No special precautions are required.

Table 8: Printing and Copying Guidelines

Restricted	Confidential	Operational	Public
• Duplication not advised; print and copy only when necessary and with approval from information owner. • Use secure print function if possible. • Unattended printing is not permitted. The person attending the printer must be authorized to view the information.	• Print only when necessary. • Copying and printing to be minimized and only when necessary. • Use secure print function if possible.	• No special precautions are required.	• No special precautions are required.

Table 9: Disposition Guidelines

Restricted	Confidential	Operational	Public
- Dispose of Restricted information only through approved secure destruction methods appropriate to the format and sensitivity of the asset. Paper records must be securely shredded or destroyed so they cannot be reconstructed. Electronic records, media, and devices must be securely sanitized, degaussed, cryptographically erased, or physically destroyed, as appropriate. Deleting, reformatting, or placing records in regular waste or recycling is not sufficient. - Disposition must be authorized, documented, and completed in accordance with retention schedules; archival records must be transferred to the Provincial Archives of New Brunswick using approved procedures.	- Dispose of Confidential information using approved secure destruction methods appropriate to the format and sensitivity of the asset. Paper records must be securely shredded or destroyed so they cannot be easily reconstructed. Electronic records, media, and devices must be securely erased, sanitized, degaussed, or physically destroyed, as appropriate. Deleting, reformatting, or placing records in regular waste or recycling is not sufficient. - Disposition must follow approved retention schedules; archival records must be transferred to the Provincial Archives of New Brunswick using approved procedures.	- Dispose of Operational information using appropriate methods based on the format and business value of the asset. Paper records should be placed in secure recycling or shredded where the information is not intended for public release. Electronic records, media, and devices should be deleted, wiped, or sanitized using approved procedures. - Disposition must follow approved retention schedules; archival records must be transferred to the Provincial Archives of New Brunswick using approved procedures.	- Dispose of Public information using routine disposal methods appropriate to the format of the asset. Paper records may be recycled or discarded through normal waste processes, and electronic records may be deleted using standard procedures. - Disposition must follow approved retention schedules; archival records must be transferred to the Provincial Archives of New Brunswick using approved procedures.

Table 9: AI Tool Data Handling Guidelines

This table applies the classification levels in Table 1 specifically to AI tools, including chat assistants, copilots, and AI agents. Where an AI tool is not listed here, apply the most restrictive applicable row until the tool has been added to the Approved Platform Guide and this table is updated.

Restricted	Confidential	Operational	Public
Not permitted. Restricted information must not be entered into an AI tool, as these tools may process, store, or expose information.	Not permitted. Confidential information must not be entered into an AI tool, as these tools may process, store, or expose information.	Information classified as Operational may be entered into NBCC-approved AI tools.	No restrictions.

AI Considerations: Tacit Knowledge and Voice/Audio Input

Tacit knowledge, institutional history, unwritten procedures, or experience that exists only in an individual's memory, is not itself classified under Table 1, since it has not been captured in any recorded form. However, once tacit knowledge is typed, dictated, or otherwise entered into an AI tool, it becomes a data asset like any other and must be classified based on its content, not its source. Before sharing institutional knowledge with an AI tool, in writing or verbally, staff should ask the same question they would ask before typing it into any other system: what classification would this receive if it were being documented for the first time?

AI tools that accept voice or audio input (including dictation, voice notes, and meeting transcription) capture more than the words spoken. They may also capture the speaker's voice itself, a biometric and personally identifying characteristic in its own right, separate from the content of what was said. Voice input should be evaluated on two dimensions:

- the classification of the content being spoken, per Table 9 above, and
- the fact that voice data may itself warrant Restricted-level handling given its biometric nature (see Table 1, "Biometric data such as fingerprints"), regardless of how innocuous the spoken content is.

This is a developing area of guidance and will be revisited as AI voice tools become more prevalent at NBCC.