NOSM UNIVERSITY | Continuing Professional Development

GUIDELINES

CPD OFFICE INFORMATION MANAGEMENT AND RECORDS RETENTION

Approval Authority: CPD Office Governance

Established: 2024 09 20

Amendments: NA

Category: Continuing Professional Development Office

1.0 STATEMENT

NOSM University (NOSM U) Continuing Professional Development Office (CPD Office) recognizes the importance of maintaining secure storage and appropriate access to sensitive and confidential information. The CPD Office Information Management and Records Retention Procedure is used in conjunction with NOSM U's Handling Sensitive Electronic Information Policy. All rights and responsibilities articulated in NOSM U's Handling Sensitive Electronic Information Policy apply along with this Procedure, and nothing in this Procedure derogates from the duties, protections and process established.

This guideline document, along with the central Handling Sensitive Electronic Information Policy, is meant to provide CPD Office stakeholders with the necessary information to meet or exceed the Professional and Legal Standards of Accreditation CPD activities as outlined by the Committee on Accreditation of Continuing Medical Education (CACME) where the following institutional accreditation standards apply:

Requirement 1.4-1

The accredited CPD provider organization uses written procedures to ensure that its governance, operations, planning processes and records management comply with applicable professional and legal standards to maintain confidentiality.

Requirement 1.4-2

The accredited CPD provider organization uses written procedures to ensure that its governance, operations, planning processes and records management comply with applicable professional and legal standards to protect privacy.

Requirement 1.4-3

The accredited CPD provider organization uses written procedures to ensure that its governance, operations, planning processes and records management comply with applicable professional and legal standards to protect copyright.

2.0 SCOPE

This guideline applies to all NOSM U CPD Office information users, whether on-campus or when accessing from a remote location.

3.0 PROCEDURES

Procedures for common types of electronic data used in CPD Office have been classified in the table below. All CPD Office Staff and stakeholders are responsible for utilizing these procedures in conjunction with the central NOSM U policy.

3.1 CPD Office Program Development Files

CPD Office Program Development files typically include application forms, approval documents, conflict of interest declarations of SPC members and speakers, certificates of attendance, presentations/handouts, evaluations, marketing, needs assessment data, speaker communication, budgets, and sponsorship contracts.

Responsibility	Classification	Storage and Distribution	Retention	Disposal
CPD Office	High-Risk	Electronic data is handled as per the NOSM U Policy	Seven (7) years after the Accreditation/Certification date	Destroy

3.2 Program Accreditation/Certification (Approval) Files

CPD OFFICE must follow the policies of the CFPC, RCPSC and CACME as they relate to the retention and destruction of program approval records and applications.

Responsibility	Classification	Storage and Distribution	Retention	Disposal
CPD Office	High-Risk	Electronic data is handled as per the NOSM U Policy	Seven (7) years after the Accreditation/Certification date	Destroy

3.3 CPD Office and Operational Files

CPD Office and Operational Files are broken down into three categories of classification.

3.3.1 CPD Office Governance Committee Files

Files typically include program committee and subcommittee terms of references, membership lists, agendas, minutes, and other meeting materials (e.g. CPD OFFICE Governance, CPD OFFICE Advisory, FPDC, and its subcommittees).

Responsibility	Classification	Storage and Distribution	Retention	Disposal

CPD OFFICE	Medium-Risk	Electronic data is handled as per the NOSM U Policy	Ten (10) years after the Accreditation/Certification date	Destroy

3.3.2 CPD Office Program Development Resource Files

Responsibility	Classification	Storage and Distribution	Retention	Disposal
CPD OFFICE	Low-Risk	Electronic data is handled as per the NOSM U Policy	Ten (10) years after the Accreditation/Certification date	Destroy

3.3.3 CPD Office General Files

CPD Office policies, procedures, guidelines, organizational charts, accreditation reports, previous survey reports, letters and other related documentation and correspondence.

Responsibility	Classification	Storage and Distribution	Retention	Disposal
CPD OFFICE	Medium-Risk	Electronic data is handled as per the NOSM U Policy	Sixteen (16) years to capture two (2) Accreditation Cycles	Destroy

3.4 CPD Office Research Data

NOSM University requires all research, innovation and scholarly inquiry conducted by its faculty, staff, and learners and under its auspices, to be performed in the most rigorous and responsible manner. All files related to research should follow the *Responsible Conduct of Research Policy* and related documents.

4.0 DEFINITIONS

Data Classification Description:
Data classification is required to determine the appropriate storage and mitigation strategies in the event of breaches and inherent risks to the University. See the Data Classification Framework for other examples relevant across the University.

High Risk:

Data that is highly sensitive and the level of protection is dictated externally by legal and/or contractual requirements.

- High-risk data may only be shared with authorized parties with a specific business need.
- **Significant Damage** would occur if high-risk data were to become available to unauthorized parties, either internal or external to NOSM U.

Examples in CPD Office may include personal information of staff, SPC members, participants in accredited activities, presentations that include patient or learner information being discussed as case presentations in CPD activities, and other information outlined in the CPD Office Privacy policy.

Medium-Risk:
Data that is not protected by law or industry regulation from unauthorized access, use, or destruction but could cause harm to NOSM U or others if released to unauthorized individuals.

- Medium-risk data may only be shared with authorized parties with a specific business need.
- **Moderate Damage** would occur if medium-risk data were to become available to unauthorized parties, either internal or external to NOSM U.

Examples in CPD Office may include proprietary information received from a third party with an expectation of confidentiality, the intellectual property of program planners and speakers (as outlined in the speaker release form completed by each speaker), registration lists with participant and community names, and research information of a non-personal, proprietary nature.

Low-Risk*:*
Data that has been approved for release to the general public and is freely shareable both internally and externally.

- Low-risk data can be shared with all parties, with or without a specific business need.
- **Minimal or No Damage** would occur if low-risk data were to become available to unauthorized parties, either internal or external to NOSM U.

Examples in CPD OFFICE may include information posted to the CPD Office websites and presentations publicly available with the signed release of speakers.

Personal Information:
Recorded information about an identifiable individual, including:

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.
b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved.
c) any identifying number, symbol or other assigned to the individual.
d) the address, telephone number, fingerprints or blood type of the individual.
e) the personal opinions or views of the individual except where they relate to another individual.
f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence that would reveal the contents of the original correspondence.
g) the views or opinions of another individual about the individual.
h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.
i) Information about an individual is not personal information unless the individual has been dead for more than thirty years.

Research and Scholarly Data:
Data collected, obtained, and used during the course of research and may be in the custody and control of the University. Includes original data, previously existing data sets, as well as the analysis, results, or dissemination resulting from the research process.

Electronic Data:
Data that is stored, transmitted, or read in an electronic format, such as a file on a drive or device, information in a database, or unstructured formats, such as email.

5.0 RELATED POLICIES

NOSM University_Policy_Handling Sensitive Electronic Information
NOSM University_Policy_Responsible Conduct of Research
NOSM University_Policy_Records Retention

6.0 INTERPRETATION

Questions of interpretation or application of this policy or its procedures will be referred to the CEPF Office at CPD Office@nosm.ca

7.0 RELATED DOCUMENTS

University Documents and Information

- NOSM University_FIPPA Policy_Information Access and Protection of Privacy
- NOSM University_FIPPA Protocol_Collection of Personal Information

- NOSM University_FIPPA Protocol_Delegation of Authority
- NOSM University_Framework_Data Classification
- NOSM University_Form_Informed Consent for Disclosure of Personal Information
- NOSM University_Form_Records Destruction
- Form_Request to Access Information

Legislation and Information

- Freedom of Information and Protection of Privacy Act
- Form_IPC Appeal
- Form_IPC Privacy Complaint

AUTHORITIES AND OFFICERS

The following is a list of authorities and officers for this guide:

a. Approving Authority: CPD Office

Review and Revision History

Review Period: 1 year or as required

Date for Next Review: 2026 09

Date	Action
2024-09-20	Approved at CPD Governance Committee
2026-06-18	Updated to reflect CPD Name Change from CEPD