

## 5.4.08 Archives and Records Management

### Operating Policy and Procedures

#### 1. **Policy**

The Navitas College of Public Safety manages information relating to students to support requirements for access to information, student progress and procedures and to meet regulatory/audit requirements. All academic student file information remains confidential except that which is placed in the public domain.

#### 2. **Purpose**

The purpose of this policy is to assure the integrity, accuracy and currency of records.

#### 3. **Responsibility**

The Student Administration Officer is responsible for compliance with this policy.

#### 4. **Guidelines**

4.1 "Record" - a record is any piece of information created or received and maintained by the Navitas College of Public Safety in the course of business or conduct of affairs and kept as evidence of such activity. Student activity forms part of this process. "Student Records" does not include statistical information based on or compiled from data which does not disclose the identity of individual students.

4.2 The Student Administration Officer has been assigned responsibility for records management of NCPS records, whether electronic or otherwise.

4.3 The release of information of an academic or personal nature relating to NCPS, past or present students other than in accordance with this policy are expressly forbidden. This includes release of information to financial agencies, police, relatives of students, etc. Any request for access to NCPS records must be authorized by the Higher Education Registrar.

4.4 Requests for information about a student from any party may be passed on to the student concerned for the student to respond if he/she wishes.

4.5 Electronic records are often housed on impermanent physical media and are subject to constant technological change. Access to information is limited when machines necessary to read these records fail and cannot be replaced. To ensure access to information, copy older formats onto a stable technology while playback machines remain available. Information in this regard is available from NCPS's information technology personnel.

#### 5. **Procedures**

##### 5.1 **Secure Storage and Backup of Electronic Records**

5.1.1 Computer disks and diskettes should be stored vertically within paper boxes. Neither the boxes nor disks should lean or slant, which causes deterioration.

5.1.2 Plastic cartridges should never be removed; nor should the cartridge shutter be opened to expose the digital optical disk's recording surface. To protect disks or tapes from warping, they should not be subject to pressure.

5.1.3 Verify a sample of electronic records weekly to ensure continued accessibility and readability.

- 5.1.4 Copies should be marked with appropriate external labels that identify the system and software used, any access restrictions, and date. Labelling is critical when the data and its index are stored on different media.
- 5.1.5 Weekly and monthly back-up copies must be stored off-site by a manager.
- 5.1.6 Do not expose electronic records to magnetic fields.
- 5.1.7 Follow the manufacturer's specifications of environmental conditions for the storage of optical disks.

## 5.2 **Retention, Archiving and Retrieval of Student Results**

- 5.2.1 Student records are maintained in hard copy for 7 years before destruction and also electronically compiled and maintained through ICARE & PEPi software on NCPS's computer systems.
- 5.2.2 Back-up of electronic records must be done daily according to procedures.
- 5.2.3 All relevant student records must be retained electronically for 30 years.
- 5.2.4 Removal of records can only be conducted under the authority of the General Manager (Public Safety).

## 5.3 **Retention, Archiving, Retrieval and Transfer of Records**

- 5.3.1 All NCPS records are maintained on the NCPS computer system;
- 5.3.2 Back-up according to procedures daily;
- 5.3.3 All records must be retained electronically for 30 years;
- 5.3.4 Transfer of records such as statistical reporting to DEEWR through the HEPCAT software must be completed according to instructions or requirements of the regulatory authority; and
- 5.3.5 Removal or transfer of records can only be conducted under the authority of the General Manager (Public Safety).

## 5.4 **External Reporting**

- 5.4.1 Transfer of records such as statistical reporting to DEEWR utilising the HEPCAT software must be completed according to instructions or requirements of the regulatory authority; and
- 5.4.2 Removal or transfer of records can only be conducted under the authority of the General Manager (Public Safety).

## 5.5 **Commercial and Confidential Information**

- 5.5.1 Records in both documented and electronic format are compiled by NCPS on a daily basis. This includes records such as minutes of meetings, reports by individuals and organisations conducting business for or on behalf of the NCPS, and trainers and lecturers. A substantial amount of these records is confidential;
- 5.5.2 All information of a commercial or confidential nature must be safeguarded and not released to unauthorised persons or entities; and
- 5.5.3 If unsure as to the commercial or confidential nature of records, the staff member must check with the Registrar before disclosure or comment.

## 5.6 **Disclosure of Client Information to Third Parties**

- 5.6.1 NCPS, through its various business activities, obtains a substantial amount of information about clients, both individual and corporate;
- 5.6.2 All information about clients must be kept confidential unless release is authorised by the client or NCPS;
- 5.6.3 Any inquiry about a client must be directed initially to the Registrar who will make a determination as to whether to contact the client or refuse the request unilaterally.
- 5.6.4 Information may be released in accordance with an authorisation signed by a student authorising the release either generally or to specific bodies or class of bodies of all or specific parts of information from the student's record. The signed authorisation should be retained on the student's file.
- 5.6.5 In the event of an accident or emergency, or a student becoming incompetent to manage his/her affairs, personal details may be released to the police, hospital, civil emergency services, or the student's legal personal representative only with the authority of the General Manager (Public Safety).

## 5.7 **Release of Information within the College**

- 5.7.1 Information relevant to the conduct and administration of College functions
- 5.7.2 The information should be restricted to information necessary for the conduct of such functions and should not normally include academic record details or personal information other than contact address and telephone number

## 5.8 **Access by Clients to Their Personal Records**

- 5.8.1 Clients are permitted under NCPS policy to access their personal records;
- 5.8.2 Any request must be in writing outlining the reason for such access. This request must then be forwarded to the General Manager (Public Safety) for a determination;
- 5.8.3 Once access is approved by the General Manager (Public Safety), the client will be permitted to view their personal record under the supervision of the Higher Education Registrar or nominee;
- 5.8.4 The client is permitted to make notes about their personal record however will not be given copies of official NCPS records unless authorised by the General Manager (Public Safety);
- 5.8.5 If the client is a student requiring copies of certificates or transcripts, the request will incur administrative fees as determined by the division concerned.

## 6. **Authority**

Authorised by the General Manager (Public Safety)

## 7. **Approved**

Approved by the Higher Education Board on 23/09/08.

**Amendments**

Date	Modified by	Sections amended/added	Approved by HEB (if required)
22/05/09	Jodie Reeve	Logo changed	Minor change
09/11/09	Christine Ashton	Change of name and logo	Minor change