Appendix B : Statement of Commitment to Confidentiality and Impartiality – Governing Principles CONF-DOC-06/2

1. **Accountability**
   All employees, managers, supervisors and faculty share a joint responsibility for the control and protection of both confidential personal information as well as any and all confidential data no matter its format.

2. **Security**
   HNCA provides appropriate safeguards for the personal information it collects. The HNCA also provides appropriate safeguards for all data, materials, products, technology, computer programs specifications, manuals, business plans, software, financial information, etc.

3. **Consent**
   HNCA will obtain an individual's consent prior to the collection, use or disclosure of his/her personal information before or at the time of interview/hire.

4. **Agreement**
   It is understood by all staff and faculty that confidential information, no matter its format, is not to be released and/or given to outside third parties unless required by provincial and/or federal law (ie. Certified Product Model and its Certificate Holder).

5. **Openness**
   HNCA is committed to making understandable the available information about policies and practices related to the management of personal and confidential information.

6. **Individual Access**
   All staff and faculty can review and verify any and all information contained in their personal files upon submitting a written request to Human Resources.

7. **Right to Privacy**
   HNCA recognizes the fundamental right of its staff and faculty to privacy with respect to their personal information and the need to ensure that the entire organization is committed to protecting all forms of confidential information in accordance with all applicable provincial privacy acts.

8. **Impartiality**
   HNCA is committed to impartiality in auditing, certification and verification activities and has the overall responsibility to ensure that all decisions are taken in accordance with the corresponding applied standards, the HNCA internal procedures and ISO 17065 requirements. HNCA does not endorse any specified consultancy organization nor imply that certification would be simpler, easier, faster or less expensive if a specified consultancy organization is used.

Special provisions for personal data protection:

1. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the HNCA shall maintain a Register through its E-Forms Requests CRM functions.
b. Individuals have the right to access their personal data and any such requests made to the HNCA shall be dealt with in a timely manner.

2. Lawful purposes

a. All data processed by the HNCA must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The HNCA shall note the appropriate lawful basis in the respective agreements / consents with individuals.
c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the HNCA's systems.

3. Data minimisation

a. The HNCA shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy

a. The HNCA shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

5. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the HNCA shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

6. Security

a. The HNCA shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

7. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the HNCA shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach the responsible authorities. This policy applies to all personal data processed by the HNCA.The Recipient shall take responsibility for the HNCA's ongoing compliance with this policy