P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA) / +599 9 523 2685 (Curacao)

Information Sharing Policy

Document version: 01-2023

Information is collected, processed, stored, shared and deleted, compliant to USA and European rules and regulations. CUN fully adheres to the European Union General Data Protection Regulation of 2018 and similar regulations for the USA, where personal information is concerned, for which the owner ('data-subject') must give his/her consent, before being collected, processed, stored or shared.

'Personal information' and 'consent' are defined according to Article 4 of the EU GDPR, as follows.

"Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

"Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

'Information' or 'data' also includes information about a person's health, physics, genetics and biometrics.

1 – Core principles

The following seven core principles govern CUN's data protection and information sharing policy.

1. Information is gathered with consent, lawfully, fairly and with transparency.
2. Information is collected and processed for a specific purpose and used only for that specific purpose.
3. The amount of information and the types of information that is collected are relative to its specific purpose and no unnecessary, redundant, irrelevant and/or superfluous information is willingly collected.
4. Information is kept accurate. Incorrect information is revised, in a timely manner and obsolete information is deleted, as soon as possible, notwithstanding personal, duty-related and study-related data that is kept as materials of proof, with the consent of the owner/data-subject.
5. Personal information is kept only for as long as needed or for as long as allowed by the owner/data-subject (the 'right to be forgotten'), notwithstanding personal, duty-related and study-related data that is kept as materials of proof, with the consent of the owner/data-subject.
6. Individuals can expect information to be collected, processed, stored and used confidentially and with integrity.
7. CUN and its students, management, faculty, staff and any other person or organization, directly related to CUN, involved in collecting, processing, storing and using information, can and will be held accountable for handling information confidentially and with integrity.

2 – Scope

Information is collected, processed, stored and shared on a regular or daily basis, as part of CUN's activities, as a business and as a nursing school. Information includes, but is not limited to student application and admission data, documents shared with CUN, during an admission process, study-related information, job application data, documents shared with CUN, during a job application process, ELCP-data, student-information shared with faculty and relevant third parties, CUN's program and course details, policies, standards, handbooks and memoranda, shared with CUN's stakeholders and relevant third parties, sharing or providing access to documents and information through CUN's electronic systems, such as SISC, its electronic libraries and e-mail and information shared with CED, CUN's Advisory Board and information

shared with its committees and councils. In these cases, information may ultimately be accessed both through CUN owned electronic devices and systems or electronic devices and systems owned by others.

3 – General stipulations

1. This policy is not limited to routine activities and includes sharing information such as research-data, both internally and externally and information shared with local authorities, in response to a legitimate request and during an immigration-process. Information sharing may also happen as part of automated ICT processes and the process-owner is responsible for ensuring that sharing complies with GDPR and CUN policies.
2. CUN's information sharing, data-protection and privacy policies are also incorporated in the Risk Assessment Procedures of all of its departments and refer to all of CUN's activities and are binding for all of CUN's students, employees, contractors, affiliates and any other person or organization receiving information from or sharing information with CUN.
3. Persons and organizations involved in sharing information with CUN receive detailed instructions for maintaining data-security and confidentiality.
4. CUN's information sharing policy applies to paper documents, as well as information stored in electronic systems and information that is shared verbally. To comply with the GDPR articles, information must be collected and used fairly, stored safely and only disclosed lawfully to third parties.
5. CUN's information sharing policy applies not only to written documents, but also to audio-files, video-files and pictures.
6. In case there is no written consent given by an owner/data-subject (person or organization), for sharing certain information with CUN, the deliberate and voluntary sharing of that information is considered to be lawfully, based on implicit consent, e.g. in case of responding to an e-mail message.
7. In case (personal) information is shared with CUN, an electronic receipt is sent by CUN to the sender of the (personal) information.
8. In case personal information is shared with CUN, by any other person or organization than the owner of that personal information him-/herself and there is no proof of consent given by the owner of that information, CUN will, if possible and feasible, contact the owner of that information to verify his/her consent. If the owner of that information does not verify his/her consent, CUN will delete the concerning information from its systems and will destroy any concerning paper documents and CUN will inform the sender of the information of its actions taken.
9. Personal information will not be stored by CUN on and CUN does not support or recommend storing any kind of CUN duty- or study-related information by others on 'cloud storage and file-sharing services', whether or not open to the general public and whether or not secured by personal login details. Such cloud storage and file-sharing facilities include 'web-mail' services (like Yahoo, Gmail, Protonmail and AOL), Google Drive, Box, DropBox, Jottacloud, iCloud, MS One Drive, MS SharePoint, iDrive, Mega, pCloud, Tresorit, Amazon (Drive), Filen, MediaFire, Degoo, Yandex Disk, UploadNow, Sync, Blomp, Internxt, Icedrive, LetsUpload, Jumpshare, TeraBox and similar services.
10. It is not allowed for personal and/or other CUN-related information, that is considered 'restricted' or 'sensitive' (see 4 – Security classification) to be shared or discussed using an electronic chat, blog or other kind of discussion platform or any kind of social media platform, not secured and managed by CUN. Such platforms include discussion and comment features on web-sites, WordPress blogs, Quora, Facebook and Facebook Messenger, Telegram, Instagram, Rocket Chat, Whatsapp, WeChat, Threema, Signal, Line, Snapchat, Skype, Google Hangouts, Viber, MS Teams, YouTube, Twitter, TikTok, Pinterest, LinkedIn and similar platforms.
11. All electronic CUN-related information that is intended to be shared, is stored on servers that are part of CUN's secure electronic network. Persons and organizations authorized by CUN to access this

information will receive instructions for use and private login details and must adhere to CUN's data protection and information sharing policies.

12. In case information is shared with persons or organizations outside the jurisdiction of the European Union or other countries adhering to the EU GDPR articles, an EU Standard Contractual Clause will be part of an Information Sharing Agreement, between CUN and that particular person or organization.
13. A record is kept (whether or not electronically) of all information that is formally shared between CUN and any other person or organization, by any means.
14. In case of an emergency (e.g. in case of an accident, where a person's health or life is in acute danger and a person is physically or mentally not able to formally consent to sharing his/her personal information or there is no time to obtain consent), personal information sharing is considered exempt from obtaining formal consent.

4 – Security classification

CUN-related information is classified on three levels.

1. Unrestricted (available for public access, like web-site content, newsletters and press-releases).
2. Restricted (available on a 'need to know' basis, such as information shared between CUN and its stakeholders and certain duty- and study-related information).
3. Sensitive (personal information, certain duty- and study-related information and CUN-information only available to persons and organizations that have received a formal authorization to access and/or receive sensitive information).

All three levels have their own security measures, based on the possible impact and consequences, in case of a security-breach, as stipulated in CUN's data-protection policies and the concerning risk assessments.

Information being kept secure on the second and third level ('restricted' and 'sensitive') can only be shared, under the following conditions.

1. A clear and unambiguous reason for sharing the concerning information, to CUN's discretion.
2. A formal authorization to share and to receive the concerning information.
3. Only parts of information-packages that are absolutely necessary to be shared, can be shared.
4. Restricted and sensitive information must be shared by providing a secure link to the concerning place of storage, on CUN's network, instead of actually sending files.

Information that is not intended to be shared (except upon request of proper authorities) is always kept secure on the third level ('sensitive').

In case of a security-breach an Information Security Incident Report (ISIR) must be filed immediately after the breach has been discovered. ISIR forms can be requested and filed at CUN's ICT Department.

4. Data-subject rights

Notwithstanding any action taken or any request made by the proper authorities and notwithstanding notable consequences of the deletion of personal and/or study-related information that is kept as materials of proof and within the limitations of relevant laws and regulations, data-subjects are granted the following rights.

1. Data-subjects have the right to have their data be sent to them or to have their data shared with any third party of their choice, at any time.
2. Data-subjects have the right to have CUN stop collecting, processing, storing and/or using their data, at any time.
3. Data-subjects have the right to have CUN delete their data, at any time.
4. Data-subjects have the right to have CUN delete the parts of their data, that is not to be considered materials of proof, as of the moment they are no longer associated with CUN.

5. Data-subjects have to right to access and/or to be formally informed about their personal data stored on CUN's electronic systems and stored in CUN's physical filing-cabinets, at any time.
6. Data-subjects have the right to revise or update their personal information or to have CUN revise or update their personal information, at any time, but with the exception of critical duty-related data and study-related information, that is kept as materials of proof.
7. Data-subjects have to right to know exactly when, where, why, how and how long their data is collected, processed, stored, shared and used otherwise.

Revision History

Date of Change	Summary of Change
January 1, 2023	