DATA PROTECTION AND DATA SECURITY POLICY

Pursuant to applicable legislation, in particular Regulation (EU) No 2016/679 of the European Parliament and of the Council to protect the privacy of individuals with regard to the processing of personal data and the free flow of such data (the "GDPR") - constitutes the following Privacy and Data Security Policy (the "Policy").

Data Controller's Name: Alfred Nobel Business College

The data controller is located at SUITE 8 TA' MALLIA BUILDINGS, Triq in- Negozju, Mriehel Industrial Zone, BKR 3000, Malta

Electronic contact of data controller: info@nobeluniv.com

Part I.
General Provisions
Purpose and principles of Regulation
1. §

(1) The purpose of this regulation is to respect the privacy of natural persons and the transparency of public affairs by enabling the exercise of the right to information and freedom of information within the institution by enabling the exercise of the right of access and disclosure of data of public interest, to ensure appropriate data security and to ensure cooperation between electronic administration.

(2) Personal data may only be processed for specified purposes, for the exercise of a right and for the performance of an obligation. At all stages of data management, the purpose of data management must be appropriate, and the recording and handling of data must be fair and lawful.

(3) Only personal data that is necessary for the fulfillment of the purpose of the data processing and suitable for the purpose may be processed. Personal data may be processed only to the extent and for the time necessary to achieve its purpose.

(4) Personal data shall be retained in the course of data management for as long as the relationship with the data subject can be restored. The data subject can be restored if the controller has the technical conditions necessary for the restoration.

(5) Data processing must ensure the accuracy, completeness and, where necessary for the purposes of data processing, the accuracy of the data and that the data subject can be identified only for the time necessary for the purposes of the data processing.

(6) Appropriate technical or organizational measures to ensure the protection of personal data should be applied in the processing of data, in particular measures to protect them against unauthorized or unlawful processing, accidental loss, destruction or damage.

(7) Access to public and non-public data and the protection of personal, classified and non-public data should be assured at all times in the course of administration.

Scope and interpretation of regulation
2. §

(1) This Policy applies to all employees of the College and to any other person involved in the College's data management activities for any reason, as well as to persons whose data are contained in the data processing activities covered by these rules and data management.

(2) The scope of these rules shall apply to all data processing or data processing activities of the College which relate to data of a natural person and which contain data of public interest or public interest, whether or not the data processing, processing is carried out fully or partly by automated means and manually.

(3) In the event of doubt, the Head of the institution shall be entitled to interpret this Code in a credible manner and, if necessary, to issue such provisions as may be necessary for its implementation.

Interpretative provisions
3. §

For the purpose of this regulation

(1) Data set 1: The totality of data managed in a single register.

(2) Data controller 2: any natural or legal person, or any entity without legal personality, which alone or jointly with others determines the purpose of the processing of data,

takes and implements the data management (including the device used) or executes with the processor.

(3) "data management": any operation or combination of operations, in particular the collection, recording, filing, storing, altering, using, retrieving, transmitting, publishing, matching or linking, blocking, deleting and destruction of data, irrespective of the procedure used, and to prevent further use of the data, taking photographs, sound or images, and recording physical characteristics that identify a person.

(4) "transfer of data" means available data to a specific third party.

(5) "data processing" means the execution of technical tasks related to the data processing operations, irrespective of the method and means used to carry out the operations and the place of application, provided that the technical task is performed on the data.

(6) data processor: any natural or legal person, or any entity without legal personality, who carries out the processing of data under a contract, including a contract under a legal act.

(7) Data Management Restriction: Locking of stored data by marking it to limit further processing.

(8) "privacy incident" means a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorized transmission or disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(9) "identifiable natural person" means a natural person who has, directly or indirectly, in particular an identity, such as a name, identification number, location data, online identification or physical, physiological, genetic, intellectual, economic, cultural or social identity of a natural person; identifiable by one or more relevant factors.

(10) "third party" means any natural or legal person, or any entity without legal personality, other than the data subject, the controller or the processor.

(11) 'recipient' means any natural or legal person, or any entity without legal personality, to whom the controller or the processor makes personal data available.

(12) Data subject: Any natural person identified or identifiable by any information.

(13) Consent: a clear, explicit and well-informed manifestation of the will of the data subject, by which he or she indicates by consent or by any other conduct expressing his or her intention to consent to the processing of personal data concerning him or her.

(14) information transfer: transmission and receipt of information between cooperating bodies.

(15) "information transfer service" means a service whereby a cooperating body transmits data or records to another cooperating body by simple or automatic transmission of information.

(16) "sensitive data" means any data falling within special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or beliefs, trade union membership, as well as genetic data, biometric identifiers for natural persons, health data and personal data relating to the sexual life or sexual orientation of natural persons.

(17) Information of Public Interest: Information or knowledge, in whatever form or by whatever means, that is owned by a public authority or other person or entity acting in the exercise of State or local government functions and any other public function as defined by law and relating to its activities or the nature of its management, its autonomous or collective nature, including in particular its powers, competencies, its organization, its professional activity and its effectiveness, the types of data held and the legislation governing its operation, as well as its management and contracts.

(18) "public interest data" means any information not covered by the definition of "public interest information", the disclosure of which, its disclosure or its disclosure are required by law in the public interest.

(19) personal data: any information relating to a data subject.

(20) protest: a statement by the data subject that he objects to the processing of his personal data and requests the termination of the data processing or the deletion of the processed data.

Part II.

Data handling

4. §

(1) Personal data may be processed if:

a) it is strictly necessary for the performance of the data controller's statutory tasks and the data subject has explicitly consented to the processing of the personal data;

b) it is ordered by law or, under the authority of the law, within the scope specified therein, in the case of data which do not qualify as special or criminal personal data, for reasons of public interest,

c) is necessary and proportionate to protect the vital interests of the person concerned or of others and to prevent or prevent an imminent threat to their life, body or property; or

d) the personal data have been explicitly disclosed by the data subject and are necessary and proportionate to the purpose of the processing.

(2) Personal data not required by law, but necessary for its proper functioning, shall be processed by the College on the basis of the consent of the data subject to the extent necessary to achieve the purpose.

(3) In the procedure initiated at the request of the data subject, at the request of the data subject, the consent shall be presumed with regard to the personal data necessary for the conduct of the proceedings.

(4) The consent of the data subject shall be deemed to have been given in respect of the personal data which he or she has provided or made public in the public domain.

(5) Particular care must be taken with regard to sensitive data. Appropriate technical and organizational measures shall be taken with regard to sensitive data to ensure that, during the processing operations, only the data strictly necessary for the performance of their task in connection with the processing operation shall be accessible.

5. §

(1) Pursuant to the principle of purpose limitation of personal data, data processed in the course of each process may only be used for the purpose of dealing with the matter, and may not be linked to other procedures or data unless the data subject has consented and exist for some personal information.

(2) During the recording and further processing of data, care must be taken to ensure the lawfulness, accuracy, completeness, timeliness and proper storage of personal data in order to prevent the data subjects' rights being violated.

(3) Unless otherwise provided by law, the College shall obtain electronically, unless otherwise provided by law, primary information from a primary source of information which is not available and may be handled by law for personal or classified information.

(4) Non-purpose-related data for which the purpose of data processing has been terminated or modified shall be destroyed immediately or at the end of the prescribed retention period. Other documents containing personal data should also be destroyed, subject to the necessary security measures. Electronically recorded data must be rendered unrecognizable and inaccessible once they have been used for their intended purpose to prevent their further use.

6. §

(1) The data subject shall have the right, in accordance with the conditions laid down by law, with respect to the personal data processed by the College:

a) to be informed of the facts relating to the processing of data prior to the commencement of the processing (hereinafter referred to as "the right to prior information");

b) upon request, make available to the controller personal data and information relating to the processing thereof (hereinafter referred to as "access"),

c) upon his / her request and in the additional cases provided for in this Chapter, his / her personal data have been rectified or supplemented by the data controller (hereinafter referred to as "the right of rectification");

d) upon your request and in the other cases provided for in this Chapter, the processing of your personal data is limited by the controller (hereinafter referred to as "the right to limit processing"),

e) upon his / her request and in the other cases provided for in this Chapter, his / her personal data shall be deleted by him / her (hereinafter "the right to erasure"),

f) institute proceedings before the Authority (hereinafter referred to as the "right of redress"); and

g) to institute court proceedings (hereinafter "the right to a judicial remedy").

(2) The College shall provide interested parties with prior information through its regulations published on its website. The mandatory content of the student enrollment form and employment contracts is the recognition by the other party that he or she has read the provision of the College's relevant regulations.

(3) The College shall keep electronic records of the data processing operations relating to the personal data under its control (hereinafter referred to as "the data controller records"). The Data Protection Officer shall ensure that the records are kept. The controller shall record:

a) the name and contact details of the controller, including each joint controller, and of the data protection officer;

b) the purposes of processing,

c) in the case of a transfer or intended transfer of personal data, the recipients of the transfer, including third country recipients and international organizations,

d) the data subjects and the data processed,

e) in the case of profiling, the fact that:

f) in the case of international transfers, the scope of the data transmitted,

g) the legal grounds for the data processing operations, including the transfer of data,

h) if known, the date of deletion of the personal data processed,

i) a general description of the technical and organizational security measures implemented in accordance with the law,

j) the circumstances surrounding the occurrence of data protection incidents in connection with the data managed by the College, their effects and the measures taken to deal with them;

k) the legal and factual reasons for any measure which restricts or refuses the data subject's access rights under this Act.

(4) The College shall keep records in accordance with these Rules in such a way as to allow the Client to electronically, within a period not exceeding 3 days, identify which data, which cooperating body, for what purpose and at what time took over.

(5) The data recorded in the data controller register shall be kept for ten years after the deletion of the processed data.

(6) If the personal data do not correspond to the reality and the correct personal data are available to the data controller, the personal data shall be corrected by the data controller.

(7) The personal data processed in accordance with the law should not be deleted at the request of the data subject.

(8) If the request for rectification, blocking or deletion of the data subject cannot be complied with, the College shall, within 25 days of receipt of the application, state in writing or with the consent of the data subject the factual and legal reasons for rejecting the application. If the application is rejected, the person concerned shall be informed of the possibility of legal redress and recourse to the Authority.

Part III.

Data protection

7. §

(1) A document or data containing personal data may be removed from the College only with the permission of the Head of Department. In this case, the employee holding the document or data carrier is responsible for its preservation, integrity and to prevent any unauthorized person from knowing its contents.

(2) Each member of staff shall carry out data management activities only to the extent necessary for the performance of their duties. The data management officer is responsible for keeping and recording the data.

(3) Records of personal data shall be kept in a closed place.

(4) Members of staff shall exercise due care in maintaining office space and equipment used for storage of documents and data. The employee must manage and store his or her

computer and the media used for it in such a way that unauthorized persons cannot access the data requiring protection. You are also required to turn off your computer at the end of your office hours and close the office door - the last employee to leave in the case of a shared office.

(5) The rules of fire protection are laid down in the College Fire Regulations.

8. §

(1) Staff may use the College's computer infrastructure only for its intended purpose.

(2) Employees are particularly required to prevent unauthorized persons from knowing their passwords to access College systems. In this context

a) passwords must be chosen in such a way that they cannot be guessed;

b) passwords should not be disclosed to others,

c) passwords should be changed at least every three months,

d) terminals and workstations accessed by a system must not leave without leaving,

e) staff members shall be prohibited from using any other person's resources in an unauthorized manner,

f) it is forbidden to break the technical barriers protecting network resources, obtain passwords from other users, or

g) it is forbidden to copy, delete or modify data and files of the system and other users outside the normal work of the employee.

(3) Both the central network and the individual workstations are protected by a firewall and regularly updated virus monitoring software, which is operated and updated by an external IT company.

(4) Physical protection of electronic data storage equipment should be ensured that:

a) they must be kept in a sheltered place,

b) eat or drink in the vicinity of computer,

c) Each employee may only remove a password protected computer from the College area, subject to strict inventory responsibility.

9. §

(1) In case of automated processing of personal data you should ensure:

a) the prevention of unauthorized input of data;

b) prevention of the use of automatic data-processing systems by unauthorized persons using data communication equipment;

c) the verifiability and identifiability of the bodies to which the personal data have been or may be transmitted using data communication equipment;

d) the verifiability and identifiability of the personal data entered into the automated data-processing systems, when and by whom;

e) the recoverability of installed systems in the event of a malfunction and:

f) the reporting of errors in automated processing.

(2) State of the art shall be taken into account when defining and applying data security measures. There should be a number of possible data management solutions that offer a higher level of protection of personal data, unless this would be a disproportionate difficulty.

Part IV.

Data request and transmission

10. §

(1) As a cooperative organization under the E-administration Act, the College shall provide electronic information to other cooperating organizations upon their legitimate request.

(2) The College shall transmit the information available from the primary and secondary sources of information electronically within 3 days of receipt of the request for such information or electronically refuse to provide the information, and the originator cooperating the body shall be informed, stating its reasons.

(3) The communication of information shall be refused if:

a) the requested information is not available to the College,

b) the information was not requested by an authorized organization through a secure connection established for that purpose,

c) the information is available elsewhere from the primary source of information.

(4) Requests for information and the transmission of information under the E-administration Act shall be made through the gateway of office.

(5) The Office of Studies and the Head of the College shall be entitled to request information and transfer information in accordance with the E-administration Act.

(6) Requests for data from the College shall be forwarded by the departments to the designated organizations and returned following the procedure using the electronic channel.

(7) The daily inspection of the office gate is the responsibility of the designated departments. The classification of incoming data requests is the responsibility of both organizational units, as appropriate. A request for a request can only be deleted from the office gate once the filing of the request and the resolution of the associated task have begun.

(8) If the information required to respond to a request received is managed by another department, the Study Department and the Head of the College shall be entitled to request information from any department. The department is required to respond to this type of internal information request within one business day. The Head of Department is responsible for the accuracy of the data and for the deadline for reply.

11. §

Any transfer of information outside the Institution other than the transfer of information under the E-Commerce Act may only be made with the prior permission of the Head of College, except for statutory or statutory disclosure of information for which the identity cannot be established.

Part V.
Data Protection Officer

12. §

(1) The College shall employ a Data Protection Officer to facilitate compliance with legal requirements regarding the processing of personal data and the rights of data subjects.

(2) A Data Protection Officer may be appointed who has an adequate knowledge of the legal requirements and the law enforcement practice relating to the protection of personal data and is capable of performing the duties involved.

(3) The College shall, in due time, involve the DPO in the preparation of any decision relating to the protection of personal data and shall provide the DPO with all the conditions, rights and resources and shall have access to all data and information necessary to carry out his duties. and necessary to keep the Data Protection Officer's professional knowledge up to date.

(4) The DPO shall facilitate the fulfillment of its obligations by the College under the legal provisions on the processing of personal data, in particular:

a) provide up-to-date information on the legal requirements governing the processing of personal data and advise the controller, the processor and the persons employed by them on the processing operations of the data;

b) continuously monitor and verify compliance with legal requirements regarding the processing of personal data, including particular legislation and internal data protection and data security policies, including clear definition of responsibilities for each data processing operation, awareness raising and awareness raising among staff involved in data processing operations; the conduct of periodic inspections;

c) facilitate the exercise of rights of the data subject, in particular by investigating data subjects' complaints and initiating actions at the controller or processor to remedy the complaint;

d) facilitate and monitor the conduct of data protection impact assessments by providing professional advice;

e) cooperate with the bodies and persons empowered to conduct the lawfulness of the processing operations and, in particular, liaise with the Authority to facilitate the prior consultation and proceedings of the Authority;

f) contribute to the drafting and modification of data protection and data security regulations.

Part VI.

Incident management

13. §

(1) The data protection incident shall be notified in writing to the data protection officer as soon as it is detected.

(2) The Data Protection Officer shall notify the Authority of the incident immediately, but no later than seventy-two hours after becoming aware of it, unless it is likely that the rights of the data subjects would not be compromised. Within the same time limit, the DPO shall investigate the incident of which he has knowledge and shall report to the Head of the College on the outcome of the investigation, the action taken or proposed.

(3) The notification to the Authority shall include:

a) the nature of the data protection incident, including, where possible, the range and approximate number of data subjects and the scope and approximate amount of data involved in the incident;

b) provide information on the name and contact details of the Data Protection Officer or of any other contact point designated for further information;

c) outline the likely consequences of a privacy incident; and

d) outline the actions taken or planned by the College to address the potential adverse consequences of the privacy incident, and other such measures.

(4) The Data Protection Officer shall, or, on the basis of the report of the Head of College, provide for him without delay

a) the replacement or correction of unlawfully damaged, altered or destroyed data, where the processing of the data is required by law or the conditions for data processing remain unchanged, or

b) terminating the possibility of unauthorized access.

(5) If a privacy incident is likely to have a material effect on the exercise of a fundamental right of the data subject, the College shall promptly inform the data subject of the incident unless:

a) the College has applied appropriate technical and organizational security measures in relation to the data affected by the data protection incident prior to

the data incident, in particular to render the data unintelligible in the event of unauthorized access, leading to its encryption;

b) the College has taken measures, following its knowledge of the data protection incident, to ensure that the consequences of the data protection incident are not such as to materially affect the exercise of a fundamental right of the data subject;

c) direct information to the data subject could only be achieved through a disproportionate effort on the part of the data controller, and the data controller shall therefore provide adequate information to the data subject in relation to the data protection incident through publicly available information; or

d) information is excluded by law.

Part VII.

Data management related to website visits

14. §

(1) The College is authorized to process certain personal data or personal data of persons visiting the Website by using the http: /nobeluniv.com website or by applying for the newsletter service through this website, in order to consent to the data subject voluntarily provided for a specific purpose. The primary purpose of data management is to make the services provided by the website more efficient, secure and personalized to the needs of the user, and to develop personalized content and statistical data when using the newsletter service. Another purpose of the College's data management is to identify users, correct errors reported while using the Website, inform users of their rights and obligations under these Rules, and handle any disputes regarding the use of the Website.

(2) The College is only authorized to use personal information provided through the website (for use of newsletter service) for direct marketing purposes only with the user's prior consent. If the user has consented to the use of his / her personal data for direct marketing purposes, such data management will extend to the withdrawal of such permission (unsubscribe from the newsletter).

(3) In addition to the personal data provided voluntarily by the user, the website may, by reason of the visit to the website, request the storage of data in the user's terminal (so-called cookie) or access to the data stored therein to deliver targeted advertising or other targeted content to a user and market research. In all cases, you must give your consent to the use of cookies by allowing the "I understand this site" icon on the Website to display this consent by using the "I understand, accept" icon; in the absence of such consent, the Website or its sub-pages may not function properly, or the User may be denied access to certain information.

Part VIII.
Transitional and final provisions

15. §

(1) Except as provided in paragraph 2, these Rules shall enter into force on 14 February 2024.

(2) Section IV of these Rules shall apply. Shall enter into force on 14.02.2024.

14/02/2024 VALETTA